Sveučilište u Zagrebu

Ekonomski fakultet

Menadžerska informatika

OKVIR UPRAVLJANJA KIBERNETIČKOM SIGURNOŠĆU ZA MALA I SREDNJA PODUZEĆA

CYBERSECURITY FRAMEWORK FOR SMALL AND MEDIUM BUSINESS

Diplomski rad

Alen Šimunic, 0067522797

Mentor: Prof. dr. sc. Mario Spremić

Zagreb, rujan, 2019.

ALEN ŠIMUNIC

Ime i prezime studenta/ice

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad

(vrsta rada)

isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Student/ica:

U Zagrebu, 10.9.2019.

(potpis)

Sažetak i ključne riječi

Razvoj digitalnih tehnologija omogućio je nove oblike poslovanja. Novo okruženje digitalne tehnologije uvjetuje intenzivnu upotrebu digitalnih tehnologija u poslovanju, a digitalna transformacija poduzeća danas je postala standard mnogih industrija. S naprednim razvojem digitalnih tehnologija otvorila su se vrata novim, sofisticiranijim i dugotrajnijim prijetnjama informacijskim sustavima. Kibernetička sigurnost postaje prva linija obrane za digitalno transformirana poduzeća. U ovom radu predstavljen je okvir za upravljanje kibernetičkom sigurnošću koji će malim i srednjim poduzećima omogućiti održavanje osnovne razine kibernetičke sigurnosti u današnjem okruženju. Rad je podijeljen u četiri konceptualne cjeline. Prva konceptualna cjelina pojašnjava pojam kibernetičke sigurnosti, njen povijesni razvoj, ulogu u korporativnom upravljanju i reviziji informacijskih sustava te način kojim se njome može upravljati. U drugoj konceptualnoj cjelini kroz digitalnu transformaciju poslovanja objasnit će se rizici koji se danas javljaju u sklopu digitalne ekonomije i predstavlja se utjecaj na razinu kibernetičke sigurnosti. Prve dvije konceptualne cjeline stvaraju podlogu za razumijevanje treće konceptualne cjeline koja predstavlja radne okvire (engl. *frameworks*) i njihovu ulogu u korporativnom upravljanju i reviziji informacijskih sustava. U toj cjelini također će se predstaviti današnji najpoznatiji okviri za upravljanje kibernetičkom sigurnošću poduzeća. Četvrta konceptualna cjelina predstavlja okvir upravljanja kibernetičkom sigurnošću za mala i srednja poduzeća (CFSMB - *Cybersecurity Framework for Small and Medium Business*). Kroz polazišne točke za izradu okvira biti će pojašnjeno zašto je CFSMB potreban danas i kako se uklapa u poslovanje poduzeća. Uz predstavljanje kompletne strukture okvira zajedno sa područjima i mjerama koje poduzeća mogu poduzeti u okviru kibernetičke sigurnosti, predstavit će se i potrebne pripreme za provedbu okvira, metodologija provedbe i kako održati kontinuitet sukladnosti s CFSMB okvirom.

Cilj rada je predstaviti izrađeni CFSMB okvir i teorijskim i obrazložiti njegovu potrebu u današnjem digitalnom okruženju. Digitalna ekonomija nema ekonomsku vrijednost bez dostupnosti digitalnih sadržaja, čime prvi prioritet digitalno transformiranih poduzeća postaje kibernetička sigurnost. CFSMB daje osnovne mjere za provođenje povećanja razine kibernetičke sigurnosti malih i srednjih poduzeća kroz tehničke, organizacijske i fizičke mjere zaštite.

Ključne riječi: kibernetička sigurnost, okvir, mala poduzeća, srednja poduzeća, sigurnost informacijskih sustava

ENGLISH

Evolution of digital technologies brought new types of business. New environment of digital technologies demands intense use of digital technologies in business and digital transformation has become a standard in many industries. With advancing development of digital technologies, a new sophisticated and long-lasting threats emerge. Cybersecurity has become a first line of defense for digitally transformed companies. Cybersecurity framework for small and medium business will be introduced in this paper, that will allow companies to maintain basic level of cybersecurity in cyberspace. It is consisted of four conceptual parts. First part explains cybersecurity, its brief historical overview, role in governance and revisions of information systems. The second part summarizes the key threats that come with digital transformation and how digital technologies allowed new vectors for cyber attacks. First two parts establish a knowledge foundation for understanding the third part that introduces frameworks. The most used cybersecurity frameworks and their methodologies will be explained in brief. Fourth and main conceptual part will introduce the CFSMB - Cybersecurity Framework for Small and Medium Business, foundational points for its development, why it is needed and how it fits in corporate strategy, as well as methods for implementation and continuous compliance.

This paper's objective is to introduce CFSMB framework, theoretical foundations and its practical usage in today's environment. Digital economy yields no value without availability of digital content, thus making cybersecurity the first priority of digitally transformed companies. CFSMB gives essential guidelines for basic cybersecurity level maintenance using technical, organizational and physical measures.

Keywords: cybersecurity, framework, small business, medium business, information systems security

Sadržaj

1 Uvod

1.1 Predmet i cilj rada

Predmet ovog rada je područje kibernetičke sigurnosti, njeno pojašnjenje, stavljanje u kontekst današnjice, isticanje važnosti i načini zaštite, s naglaskom na okvire koji se koriste kao sredstvo osiguranja adekvatne razine kibernetičke sigurnosti poduzeća.

Cilj rada je predstaviti okvir za upravljanje kibernetičkom sigurnošću za mala i srednja poduzeća (u daljnjem tekstu CFSMB - Cybersecurity Framework for Small and Medium Business). Taj okvir prvenstveno mora osigurati jednostavnost primjene uz istovremenu cjelovitost najvažnijih mjera zaštite u kibernetičkom prostoru.

1.2 Izvori podataka

Izvori podataka za izradu CFSMB-a su postojeći okviri za kibernetičku sigurnost *NIST Framework for Improving Critical Infrastructure Cybersecurity* i *CIS Controls*, uz COBIT 5 i ISO 27K obitelj standarda kao dodatne niti vodilje, a sve to uz iskustvo autora i rad s informacijskim tehnologijama i kibernetičkom sigurnošću.

1.3 Struktura i sadržaj rada

Rad je podijeljen u 4 velika poglavlja: kibernetička sigurnost, digitalna transformacija poslovanja, okviri (engl. *frameworks*) i okvir upravljanja kibernetičkom sigurnošću za mala i srednja poduzeća. U poglavlju o kibernetičkoj sigurnosti pojasnit će se razlika između informacijske i kibernetičke sigurnosti, kratka povijest i razlozi provedbe revizije informacijskih sustava i korporativnog upravljanja informatikom uz pregled najpoznatijih mjera za pomoć pri upravljanju kibernetičkom sigurnošću. U poglavlju o digitalnoj transformaciji poslovanja pojmovi digitalna ekonomija i digitalna transformacija poslovanja bit će stavljeni u kontekst današnjice s pojašnjenim rizicima koje 5 digitalnih tehnologija donose u svijet poslovanja. U poglavlju o okvirima za upravljanje informacijskom i kibernetičkom sigurnošću bit će pojašnjene osnove metodologije najpoznatijih okvira. Posljednje veliko poglavlje pod nazivom Okvir za upravljanje kibernetičkom sigurnošću za mala i srednja poduzeća (CFSMB - Cybersecurity Framework for Small and Medium Business) predstavit će okvir za upravljanje kibernetičkom sigurnošću za mala i srednja

poduzeća prilagođen današnjem okruženju i minimalnim zahtjevima kibernetičke sigurnosti, uz pojašnjenje njegovih temelja, osnovnih načela, strukture, područja, mjera, načina pripreme i metodologije provedbe te načina kontinuiranog održavanja sukladnosti s okvirom.

3 Kibernetička sigurnost

Uz sve veću konfuziju između granica informacijske i kibernetičke sigurnosti, potrebno je podvući crtu kako bi se postavili jasni temelji za razvoj okvira za upravljanje kibernetičkom sigurnošću. U ovom poglavlju, kroz definicije i usporedbe, povijesni pregled i pojašnjenje u današnjim okvirima, postavljen je pregled osnovnih informacija potrebnih za lakše razumijevanje drugih poglavlja ovog rada, a posebno samog okvira za upravljanje kibernetičkom sigurnošću.

3.1 Definicija i usporedba s informacijskom sigurnošću

Pojmovi "informacijska sigurnost" i "kibernetička sigurnost" danas se najčešće koriste kao sinonimi, posebno kod mlađih generacija koje imaju daleko veći dodir s digitalnim u usporedbi s analognim informacijama. Za potrebe razvoja okvira za upravljanje kibernetičkom sigurnošću, ta dva pojma potrebno je definirati, usporediti i poznavati njihove razlike.

Prema američkom Nacionalnom institutu za standarde i tehnologiju NIST (*National Institute for Standards and Technology*) kibernetička sigurnost je "mogućnost zaštite i obrane kibernetičkog prostora od kibernetičkih napada[1]". ISACA (*Information Systems Audit and Control Association*) pruža precizniju definiciju kibernetičke sigurnosti kao "zaštita informacijske imovine rješavajući prijetnje informacijama koje povezani informacijski sustavi obrađuju, skladište i prenose[2]".

NIST definira kibernetički prostor kao okruženje, odnosno nezavisnu mrežu informacijskih sustava koja uključuje internet, telekomunikacijske mreže, računalne sustave, softver i veze na uređaje, koja nastaje kao rezultat ljudske interakcije[3], a kibernetičke napade kao radnje unutar kibernetičkog prostora koje se odražavaju na fizički svijet[4]. NIST ovim definicijama poteže jasnu granicu kibernetičke sigurnosti kao područja usmjerenog na digitalne tehnologije i podatke. Kako je postojanje digitalnih zapisa uvjetovano postojanjem

[1] NIST (National Institute of Standards and Technology), U.S. Department of Commerce, *CSRC (Computer Security Resource Center)* [online]. Dostupno na: https://csrc.nist.gov/glossary/term/Cyber-Security [21.8.2019.]
[2] ISACA (Information Systems Audit and Control Association), Glossary [online]. Dostupno na: https://www.isaca.org/Pages/Glossary.aspx?tid=2077&char=C [21.8.2019.]
[3] NIST (National Institute of Standards and Technology), U.S. Department of Commerce, *CSRC (Computer Security Resource Center)* [online]. Dostupno na: https://csrc.nist.gov/glossary/term/cyberspace [21.8.2019.]
[4] NIST (National Institute of Standards and Technology), U.S. Department of Commerce, *CSRC (Computer Security Resource Center)* [online]. Dostupno na: https://csrc.nist.gov/glossary/term/cyberspace-attack [21.8.2019.]

fizičkih uređaja, kibernetička sigurnost zadire u fizičke komponente do one razine do koje te fizičke komponente zadiru u digitalni, kibernetički prostor. Prema Spremić, M. (2017.)[5] "Cyber-sigurnost predstavlja sve mjere kontrole i zaštite koje pojedince i kompanije štite od namjernih, sofisiticiranih i ciljanih informatičkih napada, krađe podataka i incidenata koje je teško otkriti ili spriječiti.".

Pojam "informacijska sigurnost" NIST definira kao "zaštita informacija i informacijskih sustava od neovlaštenog pristupa, korištenja, razotkrivanja, prekida, izmjena ili uništenja u svrhu pružanja povjerljivosti, cjelovitost i dostupnosti"[6]. Prema tome, informacijska sigurnost obuhvaća sve informacije (a time i podatke), neovisno o prirodi podataka, tj. neovisno o tome radi li se o fizičkom ili digitalnom prostoru. Informacijska sigurnost bavi se sigurnošću informacija i informacijskih sustava koji se temelje na tri parametra: povjerljivost (pristup informaciji ima za to ovlaštena osoba), cjelovitost (informacija je potpuna, što uvjetuje potpunost i pravilnu povezanost podataka) i dostupnost (ovlaštena osoba ima siguran i pravodoban pristup).

Pri usporedbi predstavljenih definicija, vidljivo je da postoje dodirne točke informacijske i kibernetičke sigurnosti. Oba pojma zadiru u digitalni prostor - oba pojma obuhvaćaju informacijske sustave i druge tehnologije u digitalnoj domeni, a time i digitalne informacije kojima se te tehnologije koriste. Temeljne razlike nalaze se u dodiru s fizičkom domenom - informacijska sigurnost obuhvaća i analogne informacije, dok kibernetička sigurnost zadire u fizičku domenu samo do mjere u kojoj digitalna domena utječe na nju. Spremić, M. (2017.) ukazuje na dodatne razlike između informacijske i kibernetičke sigurnosti - informatička sigurnost rutinskim i tehnološkim mjerama osigurava nižu razinu sigurnost od kibernetičke sigurnosti koja zahvaća specifične i visokosofisticirane metode napada, tj. za osnovi cilj ima sprečavanje ili ublažavanje posljedica koje stalne prijetnje, *cyber* napada i *cyber* ratova imaju na pojedince i poduzeća[7]. Spremić, M. (2017.) također navodi kako "temelj *cyber* sigurnosti više nije otkrivanje problema nego njihovo predviđanje[8]", što čini još jednu razliku u usporedbi s informacijskom sigurnošću koja najčešće fokus stavlja na

[5] Spremić, M. (2017.) *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije*, Sveučilišna tiskara d.o.o., Zagreb, str. 53

[6] NIST (National Institute of Standards and Technology), U.S. Department of Commerce, *CSRC (Computer Security Resource Center)* [online]. Dostupno na: https://csrc.nist.gov/glossary/term/information-security [21.8.2019.]

[7] Spremić, M. (2017.) *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije*, Sveučilišna tiskara d.o.o., Zagreb, str. 58

[8] Spremić, M. (2017.) *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije*, Sveučilišna tiskara d.o.o., Zagreb, str. 48

trenutačne kontrole i implementacije kontrola koje su uvjetovane postojećim problemima. Informacijska i kibernetička sigurnost zajedno rješavaju prijetnje i rizike informacijskih sustava, no tendencija kibernetičke sigurnosti jest uočavanje, predviđanje, uklanjanje i smanjenje rizika od kibernetičkih napada većeg opsega, odnosno takve prirode koja kontinuirano utječe na poslovanje i pojedince unutar poduzeća.

3.2 Kratki povijesni pregled

Povijesno gledano, informacijski su sustavi nastali istovremeno s nastankom znakovlja. Znakovi, bilo slikovni, pisani, govorni ili u bilo kojem drugom obliku, u pozadini nose informaciju. Potreba za sigurnošću informacija jasno je vidljiva iz povijesti kriptografije koja je u početku služila kao jedini način informacijske sigurnosti, dok je danas kriptografija samo mali dio informacijske sigurnosti prvenstveno zbog stvaranja digitalnog prostora u 20. stoljeću. Revizija informacijskih sustava postavila je temelje koji se i danas koriste u svrhu povećanja razine kibernetičke sigurnosti.

Revizija informacijskih sustava postaje zasebno područje izučavanja s pojavom računovodstvenih i transakcijskih informacijskih sustava. Ubrzan napredak u dostupnosti informacija uvjetovao je nastanak novog zanimanja u svijetu informacijskih tehnologija - revizor informacijskih tehnologija (*IT auditor*). Oslanjanje na pregled transakcija, računovodstvenih konta i pozicija, uvelike je doprinijelo razini kontrole i informacijske sigurnosti velikih poduzeća. Krajem 20. stoljeća važna literatura za revizore informacijskih tehnologija bila je *Model Curriculum for Information Systems Auditing* koja je razvijena u svrhu definiranja znanja i vještina koje interni revizori moraju poznavati[9].

S dodatnim razvojem interneta, kao poveznice različitih informacijskih sustava i mreža, informacijska sigurnost polako prelazi u termin kibernetička sigurnost, koji obuhvaća prvenstveno digitalni aspekt napada i zaštite, a s druge strane objedinjuje informacijske kontrole u svrhu zaštite od sofisticiranih i stalnih prijetnji informacijskim sustavima. Digitalna transformacija, koja je detaljno obrađena u sljedećem poglavlju, omogućila je dodatno izlaganje poduzeća rizicima kibernetičkog prostora premještajući temelje poslovanja poduzeća iz analognih u digitalne sfere. Kao rezultat prelaska poslovanja u kibernetički prostor, revizija informacijskih sustava nadopunjuje se korporativnim upravljanjem

[9] Senft, S., Manson, D.P., Gonzales, C., Gallegos, F. (2004.) *Information Technology Control and Audit (2nd Ed.)*, Auerbach Publications, CRC Press LLC, 2000 N.W. Corporate Blvd., Boca Raton, Florida 33431, str. 6

informatikom kako bi se zaokružilo potpuno upravljanje informacijskim tehnologijama poduzeća.

3.3 Revizija informacijskih sustava

Panian, Ž. i Spremić, M. (2007.)[10] daju opsežnu definiciju revizije informacijskih sustava: "Revizija informacijskih sustava (engl. *Information System Audit*) je sustavan postupak kojim se ocjenjuje djeluje li informatika u skladu s poslovnim ciljevima, u kojoj mjeri djelotvorno i učinkovito podupire ciljeve poslovanja i kakva je praksa (zrelost) upravljanja i kontrole informacijskih sustava na raznim hijerarhijskim razinama.".

Revizija informacijskih sustava nužna je za kvalitetno praćenje informacijskih sustava u digitalnom okruženju i upravi poduzeća daje brz i jednostavan uvid u opću razinu sigurnosti informacijskih sustava. Danas kada govorimo o informacijskim sustavima najčešće govorimo o informacijskim sustavima koji upravljaju digitalnim podacima, no informacijski sustavi koji upravljaju analognim podacima (podaci na papiru, pisane bilješke, osobni dokumenti) i dalje su od velike važnosti za normalno funkcioniranje čovječanstva. Revizija informacijskih sustava često obuhvaća i digitalne i analogne informacijske sustave, a njen temeljni cilj je provjera sigurnosti kontrola informacijskih sustava i provjera u kojoj mjeri informacijski sustavi podupiru poslovne procese, a time i poslovne ciljeve. Rezultat provedbe revizije informacijskih sustava je ocjena kvalitete informacijskog sustava, dok korporativno upravljanje informatikom pruža korak više za poduzeća koja svoje poslovanje baziraju na informacijskim tehnologijama, a što je više objašnjeno u sljedećem potpoglavlju.

3.4 Korporativno upravljanje informatikom

Za ona poduzeća koja temelje svoje poslovanje na informacijskim tehnologijama, revizija informacijskih sustava (koja prvenstveno služi za ocjenu kvalitete informacijskog sustava, razinu kojom kontrole informacijskih sustava podupiru poslovanje i sigurnost informacijskih sustava) jednostavno nije dovoljna. Prema Spremić, M. (2017.)[11] korporativno upravljanje informatikom služi za strateško povezivanje poslovanja i informatike, gdje se informacijske tehnologije gledaju kao tehnologije koje stvaraju nove i veće poslovne

[10] Panian, Ž., Spremić, M. (2007.) *Korporativno upravljanje i revizija informacijskih sustava*, Zgombić & Partneri – nakladništvo i informatika d.o.o., Zagreb, str. 22

[11] Spremić, M. (2017.) *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije*, Sveučilišna tiskara d.o.o., Zagreb, str. 190-191

vrijednosti uz poboljšanje poslovnih rezultata. Upravljanje informatičkim rizicima i stvaranje nove poslovne vrijednost digitalizacijom poslovanja dva su temeljna načela korporativnog upravljanja informatikom.

Okviri (engl. *frameworks*) danas su nezaobilazan alat u korporativnom upravljanju informatikom, pružajući mogućnost upravi i nadzornom odboru poduzeća detaljniji uvid u način na koji su informacijski sustavi uključeni u poslovanje i porast vrijednosti poduzeća.

Za razliku od revizije informacijskih sustava, korporativno upravljanje informatikom ne zadire u tehničke mjere zaštite informacijskih sustava već mjeri učinkovitost i uspješnost informacijskih sustava, stoga je za ona poduzeća čije se poslovanje temelji na digitalnim tehnologijama potrebna i sustavna revizija i korporativno upravljanje.

3.5 Načini upravljanja kibernetičkom sugurnošću

Razvojem računalstva i interneta rastao je broj, opseg i složenost prijetnji informacijskih sustava uz istovremeni rast stručnjaka i mjera koje pomažu ukloniti te prijetnje. U ovom potpoglavlju biti će navedeni samo neki od izvora koji mogu poslužiti upravljanju kibernetičkom sigurnošću poduzeća.

Standardi (norme), kao što su to ISO 27001, 27002, PCI DSS i drugi, jedan su od načina na koji poduzeća mogu pratiti svoj korak s poželjnom razinom sigurnosti industrije (engl. *benchmark*). Neki od standarda kao što su obitelj standarda ISO 27K predstavljaju upravljačke standarde, što znači da njihov cilj nije obrada direktnih tehničkih metoda zaštite, već služe kao nit vodilja u postavljanju i implementaciji strategije kojom će se tehničke metode provesti. Razlog tome je jedinstvenost informacijskih sustava. Svaki informacijski sustav za sebe je jedinstven i razlikuje se od drugog informacijskog sustava, stoga davanje smjernica tehničke prirode predstavlja problem provedbe sukladnosti, jer predložene metode u određenom okruženju ne samo da neće imati utjecaja na povećanje razine sigurnosti, već je mogu i smanjiti. Standard ISO/IEC 27001 usvojen je u hrvatskoj kao HRN 27001:2006 pod nazivom "Sustavi upravljanja informacijskom sigurnošću - Zahtjevi"[12]. Taj standard daje najbolje smjernice za stvaranje, implementaciju, provođenje, nadgledanje, provjeru, održavanje i unapređenje ISMS-a *(Information Security Management System*), sustava za upravljanje informacijskom sigurnošću poduzeća, koristeći PDCA (*"Plan-Do-Check-Act"*)

[12] Bogati, J. (2008.) *Norme informacijske sigurnosti ISO/IEC 27K, Praktični menadžment, Vol. II, br. 3*, str. 113

model. Navedeni standardi često se u praksi svrstavaju pod okvire, iako su oni zapravo standardi poslovne prakse s manje konkretnim koracima od istinskih okvira.

Kao pomoć pri upravljanju kibernetičkom sigurnošću koriste se i okviri (engl. *frameworks*). Njima se propisuju dobre prakse i preporučeni koraci za zrelije upravljanje informacijskim sustavima[13]. Najpoznatiji je takav okvir *NIST Framework for Improving Critical Infrastructure Cybersecurity* (skraćeno *NIST Cybersecurity Framework*) koji je besplatan i dostupan na poveznici https://www.nist.gov/cyberframework, što je primjereno za manja poduzeća koja nemaju veliki budžet za provedbu informacijske sigurnosti (a svoje investicije najčešće usmjeruju na softversku zaštitu), iako je sam okvir vrlo opsežan i namijenjen za velika poduzeća. *NIST Cybersecurity Framework* nastao je nakon izdavanja izvršnog naloga 13636 predsjednika Baracka Obame pod nazivom *Improving Critical Infrastructure Cybersecurity*. Odluka predsjednika potaknula je NIST prema razvoju okvira koji će omogućiti smanjenje kibernetičkih rizika kritične infrastrukture[14]. 2016. godine NIST objavljuje također besplatnu verziju okvira namijenjenu malim poduzećima pod nazivom *Small Business Information Security: The Fundamentals* dostupnu na poveznici https://www.nist.gov/publications/small-business-information-security-fundamentals. Upravo ta verzija okvira oslonac je razvoja CFSMB-a. Još jedan poznati (također besplatni) okvir pod nazivom *CIS Controls (V7.1) ili CIS CSC (Critical Security Controls),* dostupan na poveznici https://learn.cisecurity.org/cis-controls-download, također je oslonac razvoja CFSMB-a. *CIS Controls* svaku od mjera zaštite pripisuje određenoj implementacijskoj grupi: grupa 1 su mala poduzeća, grupa 2 srednja poduzeća, dok su grupa 3 korporacije[15]. *CIS Controls* naziva se kontrolnim okvirom jer manji fokus stavlja na organizacijski aspekt informacijskih tehnologija, a veći na tehničke i fizičke mjere zaštite i njihove kontrole.

Kao okvir koji prvenstveno služi za korporativno upravljanje informatikom, a dijelom obuhvaća i područje kibernetičke sigurnosti, COBIT 5, koji je izdala ISACA (*Information Systems Control and Audit Association*), zasigurno je među najpoznatijim okvirima u svijetu informacijskih tehnologija. Pojedini njegovi dijelovi služit će kao nit vodilja u razvoju CFSMB-a.

[13] Panian, Ž., Spremić, M. (2007.) *Korporativno upravljanje i revizija informacijskih sustava*, Zgombić & Partneri – nakladništvo i informatika d.o.o., Zagreb, str. 17

[14] https://www.nist.gov/cyberframework/new-framework [21.8.2019.]

[15] Center for Internet Security (2019.) *CIS Controls* [PDF]. Dostupno na: https://www.cisecurity.org/controls/

Nacionalne strategije još su jedan od izvora informacija koje mogu pomoći u razvoju i provedbi strategije kibernetičke sigurnosti. Sjedinjene Američke Države 2011. godine izdale su *International Strategy for Cyberspace*. Hrvatska je 2015. godine usvojila Nacionalnu strategiju kibernetičke sigurnosti Republike Hrvatske koja je besplatna i dostupna na poveznici https://www.uvns.hr/en/information-security-290/cyber-security. Nacionalne strategije nisu usmjerene prema poduzećima, već prema javnom sektoru, no mnoge smjernice mogu poslužiti za razvoj strategije kibernetičke sigurnosti poduzeća.

Česte su i smjernice raznih poduzeća i istraživačkih instituta. Jedan od primjera je *Consensus Audit Guidelines* (CAG) koji predstavlja 20 smjernica za kritične kontrole kibernetičke sigurnosti prvenstveno za javni sektor, ali i za velike sektore kao što su sektor financija i sektor bankarstva. Smjernice su besplatne i dostupne na poveznici https://www.sans.org/critical-security-controls. *International Chamber of Shipping* izdala je *Guidelines on Cyber Security Onboard Ships*, skup smjernica koje služe održavanju adekvatne razine kibernetičke sigurnosti na velikim brodovima. Te su smjernice također besplatne za javnost, što je odlično za manja i srednja poduzeća, a dostupne su na poveznici http://www.ics-shipping.org/free-resources/safety-and-operations.

4 Digitalna transformacija poslovanja

Kao najnoviji trend poslovanja poduzeća u digitalnom okruženju javlja se digitalna transformacija poslovanja. U ovom poglavlju biti će pojašnjeni pojmovi digitalne transformacije poslovanja i digitalne ekonomije, biti će predstavljene digitalne tehnologije i osnovni rizici koje sa sobom donose u poslovno okruženje.

4.1 Definicije i povijesni pregled

Kroz evoluciju primjene informatike u poslovanju, koju predstavljaju Panian, Ž. i Spremić, M. (2007.)[16], informatika se prvo javlja kao tehnološka infrastruktura u svrhu podrške rutinskim poslovima, bazama podataka, umrežavanju računala i sličnim danas baznim tehnologijama koje posjeduje svako poduzeće. Daljnji napredak doveo je do uloge informatike kao sredstva povezivanja (često u komunikaciji kroz sve razine poduzeća,

[16] Panian, Ž., Spremić, M. (2007.) *Korporativno upravljanje i revizija informacijskih sustava*, Zgombić & Partneri – nakladništvo i informatika d.o.o., Zagreb, str. 9

izvještavanje i slične radnje) i kao temelj pružanja digitalnih usluga. Nakon toga informatika postaje strateški resurs poslovanja i javlja se korporativno upravljanje informatikom koje osigurava da se informacijske tehnologije koriste učinkovito i uspješno, a sve u svrhu povećanja vrijednosti poduzeća. Danas, kao rezultat digitalne transformacije poslovanja, postoje poduzeća koja se u potpunosti temelje na informacijskim tehnologijama. Takva poduzeća jednostavno ne mogu obavljati svoje temeljno poslovanje bez postojanja informacijske tehnologije. U takvom digitalnom okruženju, rizik od napada na informacijsku tehnologiju poduzeća u potpunosti postaje rizik od gubitka poslovanja poduzeća, a revizija informacijskih sustava i korporativno upravljanje informatikom postaju svakodnevni posao takvih poduzeća.

Spremić, M. (2017.) detaljno obrađuje temu digitalne transformacije poslovanja definirajući digitalnu transformaciju poslovanja kao "intenzivnu primjenu digitalne tehnologije i digitalnih resursa u svrhu stvaranja novih izvora prihoda, novih poslovnih modela i, općenito, novih načina poslovanja"[17], a kao okruženje digitalno transformiranih poduzeća definira pojam digitalne ekonomije kao "krovni pojam za označavanje novih modela poslovanja, proizvoda, usluga, tržišta i brzorastućih sektora ekonomije, posebice onih koji se temelje na digitalnim tehnologijama kao osnovnoj infrastrukturi poslovanja"[18]. Također navodi 5 temeljnih digitalnih tehnologija: mobilne tehnologije, društvene mreže, računalstvo u oblacima, veliki podaci i senzori i internet stvari[19].

4.2 Rizici poslovanja poduzeća u okviru digitalne ekonomije

Uvođenje novih digitalnih tehnologija danas je gotovo neizbježno za poslovanje većine poduzeća. Digitalna transformacija poslovanja, uz otvaranje novih poslovnih prilika, otvorila je dodatna vrata zlonamjernim ekspertima za informacijske sustave, tzv. *hakerima*. Svaka od 5 digitalnih tehnologija na kojima se temelji digitalna ekonomija nosi svoje rizike i prijetnje, od kojih će ovdje biti navedeni samo neki, osnovni rizici i prijetnje, koje CFSMB nastoji ublažiti.

Mobilne tehnologije (engl. *mobile technologies*) omogućile su da svaka osoba na svijetu na dlanu svoje ruke ima računalo koje je u nekim slučajevima bolje konfiguracije od stolnog računala koje ta osoba ima kod kuće. Sa strane korisničkog iskustva, nastaje težnja

[17] Spremić, M. (2017.) *Digitalna transformacija poslovanja*, Sveučilišna tiskara d.o.o., Zagreb str. 38
[18] Spremić, M. (2017.) *Digitalna transformacija poslovanja*, Sveučilišna tiskara d.o.o., Zagreb str. 20
[19] Spremić, M. (2017.) *Digitalna transformacija poslovanja*, Sveučilišna tiskara d.o.o., Zagreb str. 21

utopiji da u svega nekoliko milisekundi stvorimo pristup apsolutno svakoj informaciji ili odradimo neku akciju, dok sa strane kibernetičke sigurnosti porast brzine procesiranja podataka i raznolika povezivost uređaja znači povećani broj ulaznih i izlaznih vektora za zloćudne napade, kao i brzina odvijanja napada zloćudnog softvera unutar aplikacija i operativnog sustava uređaja. Tehnologije kao bluetooth i 5G sa sobom nose bolju povezanost uređaja, ali s time i konzistentniju mrežu vektora za napad zloćudnih softvera.

Društvene mreže (engl. *social networks*) danas predstavljaju svakodnevicu. Dnevna prijava nekoliko puta i stalna komunikacija putem društvenih mreža postala je društveni standard. Koliko čovječanstvu odgovara dostupnost i proširenost osobnih podataka, toliko se osobni podaci mogu koristiti kao pomoć u kibernetičkom ratovanju (engl. *cyber warfare*). Sve češće korištenje kamere i biometrijskih podataka napadačima često daje uvid ili pristup onim podacima koji mogu omogućiti da povežu informacije i saznaju tko je osoba koja je u nekom poduzeću zaslužna za očuvanje kibernetičke sigurnosti, gdje drži svoje računalo, kada koristi računalo, kako se tom računalu može pristupiti (prema marki, modelu, operacijskom sustavu i softverima) i slično.

Računalstvo u oblacima (engl. *cloud computing*) danas je gotovo nezaobilazno i samom primjenom svih drugih digitalnih tehnologija koristimo računalstvo u oblacima. Dostupnost računalnih resursa putem interneta (engl. *Infrastructure as a Services - IaaS*) istovremeno otvara vektore napada na internetom povezana virtualna računala koja su često ostavljena *online* bez adekvatnog nadzora i kontrole. *Indie* programeri često u stvaranju aplikacija (pogotovo u razvojnoj i beta fazi) stvaraju brojna virtualna računala u oblacima bez redovnog nadzora i kontrole, samo kako bi što prije izbacili aplikaciju na tržište.

Veliki podaci (engl. *big data*) usavršili su neke od najpoznatijih *online* platformi kao što su Alibaba, Amazon, Netflix, Facebook, Instagram, Twitter, eBay i druge. Tehnologije obrade velikih podataka osigurale su brzu pohranu, kategorizaciju, klasifikaciju, obradu i analitiku velikog opsega raznolikih podataka. Velika količina podataka za napadače znači da na jednom ili relativnom malom broju mjesta mogu s nekoliko napada prikupiti gotovo sve podatke o korisnicima neke platforme. Centri podataka postali su glavna meta napadača, jer iako je malo uspješnih napada, samo je jedan uspješni napad potreban za dobivanje velike količine podataka koji se mogu prodati na crnom tržištu.

Senzori i internet stvari (engl. *Internet of Things - IoT*) danas su jedan od najlakših ulaznih vektora zloćudnog softvera. Velika količina uređaja s premalom procesorskom

snagom za antivirusnu zaštitu (a često rade i bez nje) otvara milijune potencijalnih vektora za napad gdje napadači često i ne moraju probijati zaštitu jer same zaštite nema. Razlog zašto nema dovoljno procesorske snage za antivirusnu zaštitu leži u razvoju visoko specijaliziranih uređaja koji često na vlastitoj bateriji moraju mjesecima prikupljati podatke iz senzora i vršiti obradu i slanje tih podataka na poslužitelje koji te podatke dalje pohranjuju u baze podataka. Raspberry Pi, Arduino i micro:bit neki su od najpoznatijih računala za internet stvari. Česti vektor za napad je USB otvor uređaja koji najčešće nema nikakvu zaštitu i napadač može preuzeti kontrolu nad izvornim kôdom uređaja i slati/primati podatke sa poslužitelja s kojima je uređaj povezan. Temeljna zaštita uređaja koji su dio interneta stvari leži u fizičkoj zaštiti uređaja gdje se napadaču nastoji fizički prepriječiti pristup do uređaja.

5 Najpoznatiji okviri za upravljanje kibernetičkom sigurnošću i njihove metode

Prema istraživanju *Trends in Security Framework Adoption*[20] poduzeća Dimensional Research 2016. godine, 84% ispitanih organizacija u Sjedinjenim Američkim Državama koristi neki od okvira za kibernetičku sigurnost u svom poslovanju, s time da je najveći broj organizacija koji koristi neki okvir iz bankovne i financijske industriji, dok je najveći broj organizacija koje ne koriste nikakav okvir u medicinskoj i zdravstvenoj industriji. 16% ispitanika iskazalo se da njihova organizacija ne koristi nikakav okvir za kibernetičku sigurnost.

Istraživanje je pokazalo da su četiri najkorištenija okvira za kibernetičku sigurnost (uz napomenu da 44% organizacija istovremeno koristi više od jednog okvira):

1. PCI DSS (47%),
2. ISO 27001/27002 (35%),
3. *CIS Critical Security Controls* (32%) i
4. *NIST Framework for Improving Critical Infrastructure Cybersecurity* (29%).

U ovom poglavlju ukratko će biti predstavljene metodologije PCI DSS, *CIS Critical Security Controls* i *NIST Framework for Improving Critical Infrastructure Cybersecurity*, s fokusom na informacije od ključne važnost za razvoj CFSMB-a.

5.1.1 PCI DSS

PCI DSS stoji kao skraćenica za *Payment Card Industry Data Security Standard* - skup standarda za postavljanje adekvatne razine sigurnosti za sudionike industrije kartica za plaćanje. Ovaj se standard smatra obavezom svih sudionika kartičarske industrije, s aktualnom verzijom 3.2.1. izdanom u 5. mjesecu 2018. godine, a sastoji se od 6 dijelova s ukupno 12 uvjeta koje organizacija mora ispuniti:

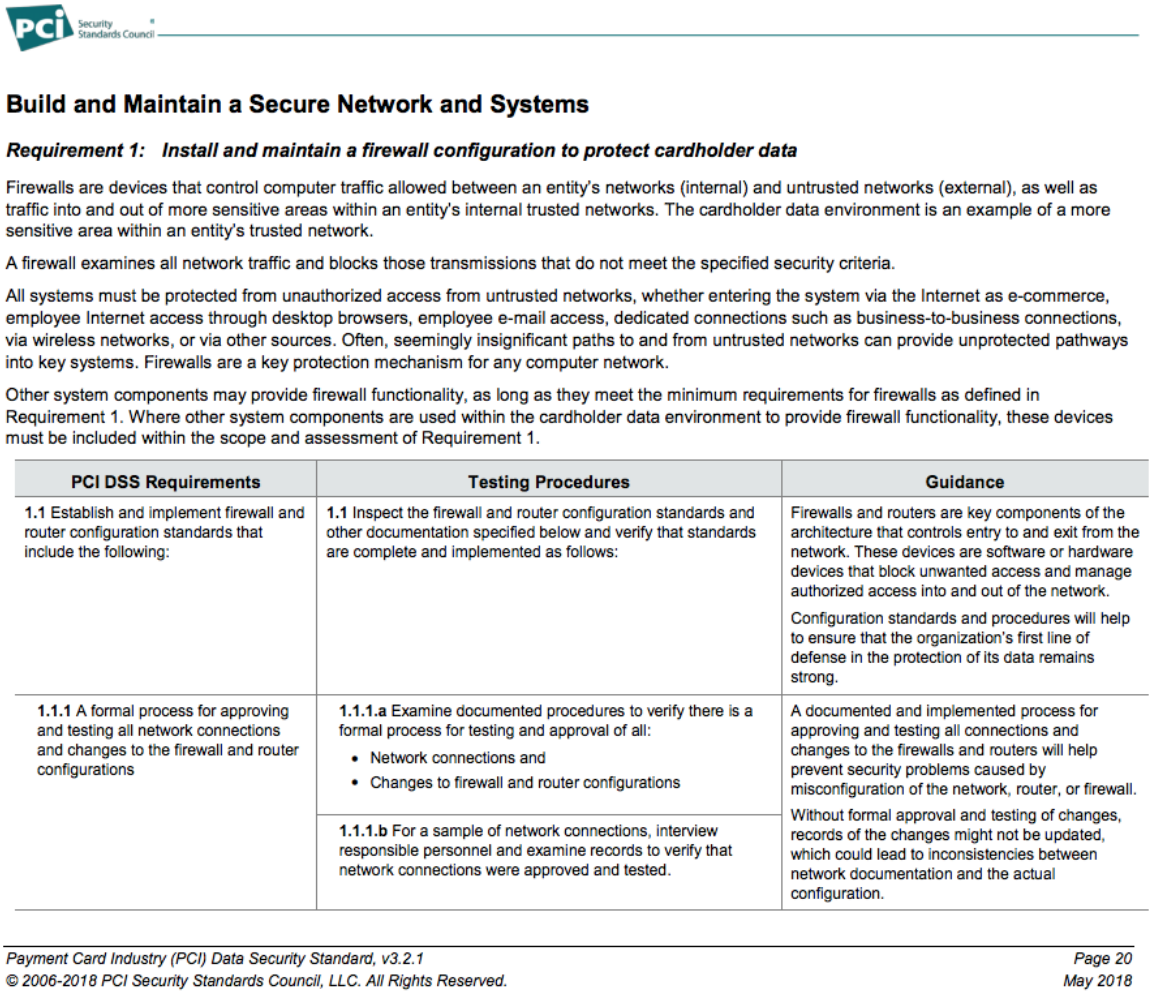
1. izgraditi i održavati sigurnost mreža i sustava:
    a. instalirati i održavati postavke vatrozida u svrhu zaštite podataka vlasnika kartice,

[20] Dimensional Research (2016.) *Trends in Security Framework Adoption* [PDF]. Dostupno na: https://www.tenable.com/whitepapers/trends-in-security-framework-adoption

b. nemojte koristiti unaprijed postavljene postavke proizvođača za lozinke sustava i drugih sigurnosnih parametara,

2. štititi podatke vlasnika kartica:
    a. štititi pohranjene podatke vlasnika kartica,
    b. enkriptirati podatke vlasnika kartica u prijenosu preko otvorenih, javnih mreža,
3. održavati program upravljanja ranjivostima:
    a. štititi sve sustave od zloćudnog softvera i učestalo ažurirati antivirusni softver ili programe,
    b. razviti i održavati sigurne sustave i aplikacije,
4. implementirati stroge mjere kontrole pristupa:
    a. ograničiti pristup podacima vlasnika kartica na *need-to-know* razinu,
    b. identificirati i autenticirati pristupe sustavskim komponentama,
    c. ograničiti fizički pristup podacima vlasnika kartica,
5. učestalo nadgledati i testirati mreže:
    a. pratiti i nadgledati sve pristupe mrežnim resursima i podacima vlasnika kartica,
    b. učestalo testirati sigurnosne sustave i procese,
6. održavati politiku zaštite informacija:
    a. održavati politiku koja zahvaća informacijsku sigurnost cijelog osoblja.

Kako se PCI DSS prvenstveno odnosi na kartičarsku industriju, njegov značaj za razvoj CFSMB-a je malen u usporedbi s NIST-ovim okvirom ili *CIS Controls*, no sigurnosne mjere, protokoli i procesi zaštite poslužiteljske infrastrukture koristit će se u razvoju CFSMB-a.



Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

PCI DSS Requirements	Testing Procedures	Guidance
1.1 Establish and implement firewall and router configuration standards that include the following:	**1.1** Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:	Firewalls and routers are key components of the architecture that controls entry to and exit from the network. These devices are software or hardware devices that block unwanted access and manage authorized access into and out of the network. Configuration standards and procedures will help to ensure that the organization's first line of defense in the protection of its data remains strong.
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	**1.1.1.a** Examine documented procedures to verify there is a formal process for testing and approval of all: • Network connections and • Changes to firewall and router configurations	A documented and implemented process for approving and testing all connections and changes to the firewalls and routers will help prevent security problems caused by misconfiguration of the network, router, or firewall. Without formal approval and testing of changes, records of the changes might not be updated, which could lead to inconsistencies between network documentation and the actual configuration.
	1.1.1.b For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested.	

Slika 1, Ekranski prikaz PCI DSS[21]

5.1.2 NIST Framework for Improving Critical Infrastructure Cybersecurity

Aktualna verzija NIST-ovog okvira je verzija 1.1, izdana 16.4.2018.. Kao što i naziv govori, ovaj NIST-ov okvir namijenjen je za upravljanje kibernetičkim rizicima kritične infrastrukture. Prema definiciji iz okvira, kritična infrastruktura predstavlja sustave i imovinu, bilo fizičku ili virtualnu, toliko važnu da bi prestanak funkcioniranja ili uništenje imalo za posljedicu smanjenje nacionalne sigurnosti, ekonomije, javnog zdravstva i sličnih infrastruktura. Iako je okvir namijenjen prvenstveno kao zaštita kritične infrastrukture, svakako je primjenjiv i na ostatak infrastrukture organizacije. Okvir se sastoji od 3 sastavna dijela:

[21] PCI Security Standards Council, LLC (2018.) *Payment Card Industry (PCI) Data Security Standard* [PDF]. Dostupno na: https://www.pcisecuritystandards.org/document_library?document=pci_dss

1. *Framework Core* - set kibernetičkih aktivnosti, željenih ishoda i primjenjivih referenca koje su zajedničke sektorima kritične infrastrukture, a predstavljene su kroz 5 funkcija (svaka sadrži kategorije i podkategorije):
    a. *Identify* - upravljanje imovinom, poslovno okruženje, korporativno upravljanje, procjena rizika i strategije upravljanja rizicima,
    b. *Protect* - upravljanje identitetima i pristupima, edukacija zaposlenika, sigurnost podataka, zaštita informacija i procesa, održavanja, tehnologije zaštite,
    c. *Detect* - anomalije, događaji, kontinuirano praćenje sigurnosti, proces otkrivanja,
    d. *Respond* - plan odgovora, komunikacije, analize, smanjenje rizika, poboljšanje,
    e. *Recover* - plan oporavka, poboljšanje, komunikacije,
2. *Framework Implementation Tiers* - predstavlja kontekst u kojem organizacija upravlja rizicima kroz 4 reda (svaka organizacija trebala bi nastojati ići iz manjeg u viši red):
    a. *Tier 1* - djelomično upravljanje rizicima (najčešće *ad hoc*, tj. stihijski),
    b. *Tier 2* - razina dobre informiranosti o rizicima (no bez konkretnih koraka),
    c. *Tier 3* - ponavljajuće upravljanje rizicima (prilagodba novonastalim praktičnim smjernicama i drugim okvirima),
    d. *Tier 4* - prilagodljivo upravljanje rizicima (mogućnost predviđanja i prilagođavanja prijetnjama i rizicima),
3. *Framework Profile* - određenje profila koji omogućavaju organizaciji procjenu trenutačnog stanja i postavljanje željene razine sukladnosti s okvirom.

U sklopu okvira predstavljeni su i koraci za uspostavljanje ili unapređenje programa kibernetičke sigurnosti organizacije:

1. postavljanje prioriteta i opsega obuhvata,
2. orijentacija (konzultacija s izvorima kako bi se saznale prijetnje i ranjivosti),
3. stvaranje trenutačnog profila,
4. provedba procjene rizika,
5. stvaranje ciljanog profila,
6. određivanje, analiziranje i prioritiziranje raskoraka (trenutačnog od ciljanog profila) i
7. implementacija i akcijski plan.

NIST okvir sadrži i dodatke koji su od ključne važnosti za provedbu i razumijevanje okvira:

1. dodatak A - *Framework Core* u tabličnom obliku s funkcijama, kategorijama, podkategorijama i referencama,
2. dodatak B - pojmovnik odabranih pojmova i
3. dodatak C - lista akronima korištenih u okviru.

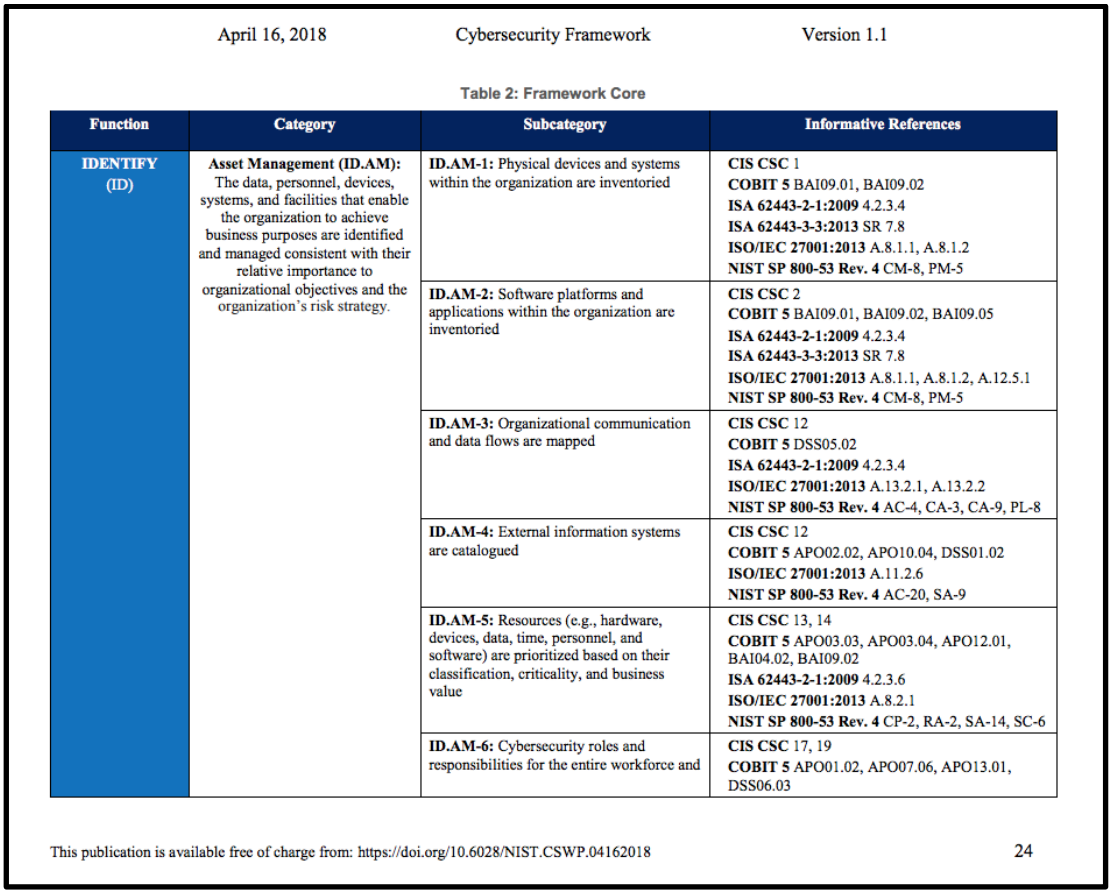
Ključan dio NIST-ovog okvira predstavlja dodatak A: jezgra okvira (engl. *Appendix A: Framework Core*) gdje su u tabličnom obliku prikazane funkcije, njihove kategorije, podkategorije i informativne reference (veze na druge okvire i dokumente gdje se mogu pročitati konkretne smjernice). Iz informativnih referenci vidljivo je da se NIST-ov okvir oslanja i na druge okvire i dokumente, kao što su *CIS Controls*, COBIT 5, ISA 62443-2-1, ISA 62443-3-3, ISO 27K obitelj standarda i NIST SP 800. Obzirom na obuhvat i iscrpnost informacija, nije iznenađujuće što danas većina organizacija u svijetu teži prvenstveno sukladnosti s NIST-ovim okvirom, a tek onda sukladnosti s drugim okvirima i standardima.

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Slika 2, NIST funkcije



April 16, 2018 Cybersecurity Framework Version 1.1

Table 2: Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018 24

Slika 3, NIST dio funkcije IDENTIFY

5.1.3 CIS Critical Security Controls

Skraćeno se još naziva i *CIS CSC* ili *CIS Controls*. Aktualna verzija 7.1. izdana 1.4.2019. daje pregled 20 najvažnijih kontrola kibernetičke zaštite:

1. popis i kontrola hardvera,
2. popis i kontrola softvera,
3. stalno upravljanje ranjivostima,
4. kontrola korištenja administrativnih ovlasti,
5. sigurna konfiguracija hardvera i softvera na mobilnim uređajima, prijenosnim računalima, radnim stanicama i poslužiteljima,
6. održavanje, nadzor i analiza zapisa rada sustava,
7. zaštita e-pošte i web preglednika,
8. zaštita od zlođudnog softvera,
9. ograničena upotreba i kontrola mrežnih portova, protokola i usluga,
10. sposobnost povrata podataka,

11. sigurne konfiguracije mrežnih uređaja poput vatrozida, usmjernika i prespojnika,
12. zaštita vanjskih dijelova mreže,
13. zaštita podataka,
14. kontrola pristupa uz *need-to-know* politiku,
15. kontrola bežičnog pristupa,
16. nadzor i kontrola korisničkih računa,
17. implementacija programa edukacije o sigurnosti,
18. sigurnost aplikativnog softvera,
19. upravljanje sigurnosnim incidentima i
20. penetracijski testovi i uvježbavanje izvanrednih situacija.

CIS Controls za svaku mjeru označava koja je implementacijska grupa treba provesti. Implementacijska grupa 1 predstavlja organizacije s ograničenim resursima i ekspertima kibernetičke sigurnosti (najčešće male i srednje organizacije), implementacijska grupa 2 predstavlja organizacije s dostupnim resursima i ekspertima (najčešće srednje organizacije) i grupa 3 predstavlja organizacije koje raspolažu s velikom količinom resursa i stručnjaka (najčešće velike organizacije, tj. korporacije). Model implementacijskih grupa biti će primijenjen i u CFSMB-u kako bi se olakšala provedba malim poduzećima i fokus na najbitnije mjere. *CIS Controls* nasljeđuje funkcije iz NIST-a i uz svaku mjeru definira tip imovine (ukoliko je moguće).

Implementation Group 1
An organization with limited resources and cybersecurity expertise available to implement Sub-Controls

Implementation Group 2
An organization with moderate resources and cybersecurity expertise to implement Sub-Controls

Implementation Group 3
A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls

CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups		
					1	2	3
9.1	Devices	Identify	Associate Active Ports, Services, and Protocols to Asset Inventory	Associate active ports, services, and protocols to the hardware assets in the asset inventory.		●	●
9.2	Devices	Protect	Ensure Only Approved Ports, Protocols, and Services Are Running	Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system.		●	●
9.3	Devices	Detect	Perform Regular Automated Port Scans	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.		●	●
9.4	Devices	Protect	Apply Host-Based Firewalls or Port-Filtering	Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
9.5	Devices	Protect	Implement Application Firewalls	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.			●

Slika 4, CIS Control dio područja 9

6 Okvir upravljanja kibernetičkom sigurnošću za mala i srednja poduzeća (CFSMB - Cybersecurity Framework for Small and Medium Business)

6.1 Polazišne točke za izradu okvira

U sljedećim potpoglavljima predstavljene su polazišne točke za izradu okvira za upravljanje kibernetičkom sigurnošću, prvenstveno u svrhu upoznavanja sa pozadinskim namjerama izrade okvira i kako bi se omogućio kratki uvid u strukturu okvira.

6.1.1 Mala i srednja poduzeća

U prethodnim poglavljima navedeni su neki od poznatih okvira za upravljanje informacijskom sigurnošću. Takvi okviri često su namijenjeni za velika poduzeća (korporacije, grupacije, multinacionalne kompanije). U nedostatku okvira za upravljanje informacijskom sigurnošću malih i srednjih poduzeća (posebno na hrvatskom jeziku), CFSMB nastoji poslužiti kao okvir koji će mala i srednja poduzeća pripremiti za temeljne rizike u kibernetičkom prostoru današnjice.

Iako mala poduzeća često nemaju dovoljno kapitalnih i ljudskih potencijala za provedbu mjera informacijske sigurnosti, CFSMB će za mala poduzeća na razumljiv i jednostavan način omogućiti provedbu i osiguranje osnovne zaštite u kibernetičkom prostoru. Kako srednja poduzeća nose dodatne rizike, u CFSMB okviru svaka će mjera imati oznaku koja ukazuje na to treba li tu mjeru provesti u malom i/ili srednjem poduzeću, a pripreme za provedbu okvira, metodologiju provedbe okvira i kontinuitet održavanja sukladnosti s okvirom će imati razdvojene upute za mala i srednja poduzeća.

6.1.2 Kibernetička sigurnost, temeljni okviri i standardi

Obuhvaćanje cijele informacijske sigurnosti u jedan okvir rezultiralo bi mogućnosti za veću razinu informacijske sigurnosti svih poduzeća koja se odluče na provedbu CFSMB-a, no za mala i srednja poduzeća pokrivanje kibernetičke sigurnosti trebalo bi predstavljati osnovnu zaštitu u kibernetičkom prostoru današnjice. Fokus na samo kibernetičku sigurnost, kao dio informacijske sigurnosti, olakšava provedbu i održavanje sukladnosti uz osiguranje osnovne razine zaštite.

CFSMB se utemeljuje na NIST okviru i *CIS Controls* dok se nadopunjuje smjernicama iz COBIT 5 i ISO 27K obitelji standarda. Svaka mjera koja se temelji na nekoj od smjernica drugog okvira u opisu će imati navedeno na kojoj se smjernici kojeg okvira temelji.

6.1.3 Struktura okvira

CFSMB dijeli se na 4 cjeline:

1. pregled okvira,
2. pripreme za provedbu okvira,
3. metodologija provedbe okvira i
4. kontinuitet održavanja sukladnosti s okvirom.

Pregled okvira predstavlja potpuni Okvir upravljanja kibernetičkom sigurnošću za mala i srednja poduzeća (CFSMB) koji se dijeli na područja koja sadrže mjere za provedbu sukladnosti s okvirom. Svaka od mjera ima oznaku na koju se veličinu poduzeća primjenjuje.

Pripreme za provedbu okvira pružaju informacije o načinu predstavljanja okvira upravi i koordinaciju za provedbu okvira u dogovoru s upravom poduzeća. Kako mala poduzeća često imaju upravu koja se sastoji od samo jedne osobe (ili u slučaju obrta gdje nema uprave), za mala poduzeća ovaj dio predstavlja opće naputke koji omogućavaju bolju organizaciju poslova prilikom provedbe i kontinuiteta održavanja sukladnosti s okvirom.

Metodologija provedbe okvira nastoji dati uvid u smjernice prilikom provedbe sukladnosti s okvirom. Predložene smjernice nisu uvjet za ispravnu provedbu sukladnosti i osobe koje provode sukladnost ne moraju se nužno držati predloženih smjernica, pogotovo ako su u sukobu s internim politikama poduzeća.

Kontinuitet održavanja sukladnosti s okvirom postavlja nekoliko ključnih smjernica na koji se način može održavati sukladnost s okvirom i na taj način predstavlja skup poslova koje je potrebno dodijeliti odabranim osobama kako bi se pobrinule da poduzeće i dalje održava zadovoljavajuću razinu kibernetičke sigurnosti.

6.1.4 Područja

CFSMB nasljeđuje osnovnu strukturu NIST okvira i sastoji se od 5 područja:

1. A - Identifikacija,
2. B - Zaštita,
3. C - Otkrivanje,
4. D - Odgovaranje i
5. E - Oporavak.

6.1.4.1 A - Identifikacija

U ovom području generalni cilj jest dobivanje strukturne slike poduzeća. Kroz popisivanje imovine (hardvera i softvera), kritičnih podataka, ljudskih potencijala i procjene rizičnosti, točno će biti određeni predmeti provedbe sukladnosti s CFSMB-om.

6.1.4.2 B - Zaštita

Prema popisima i dijagramima iz područja A, za svaku stavku potrebno je provjeriti jesu li zadane kontrole prisutne i aktivne. U ovom području bitno je definirati tko će, na koji način, prema kojim uputama i koliko često provoditi provjeru zaštite imovine i podataka.

6.1.4.3 C - Otkrivanje

Prolaskom kroz ovo područje organizacija će odrediti na koji način će detektirati prijetnje njezinim informacijskim sustavima. Također je bitno definirati tko će, na koji način, prema kojim uputama i koliko često provoditi mjere detekcije.

6.1.4.4 D - Odgovaranje

Smjernice iz ovog područja pomoći će u definiranju odgovora na određenu aktivnu ili neaktivnu prijetnju. Odgovor na prijetnju ima za cilj ili uklanjanje aktivne prijetnje ili uklanjanje rizika od aktivacije neaktivne prijetnje.

6.1.4.5 E - Oporavak

Poduzeće mora imati ažuran i zaposlenicima poznat plan oporavka od velikih napada na kritičnu infrastrukturu informacijskog sustava. Kroz ovo područje poduzeće će definirati planove oporavka i ojačanja postojeće zaštite informacijskog sustava.

6.1.5 Mjere

Svako od područja CFSMB-a ima svoje mjere koje se u sklopu tog područja poduzimaju. Mjera ne mora nužno predstavljati mjeru prema definiciji, već može predstavljati

i opću smjernicu. Svaka mjera uz sebe ima oznaku odnosi li se na malo i/ili na srednje poduzeće. Dodatni naputci uz svaku mjeru služe kao dodatno pojašnjenje kako se mjera provodi, ponekad i uz konkretan primjer provedbe mjere. Gdje je potrebno, mjera ima iskazane najveće rizike ne provedbe mjere, pod skraćenim nazivom RNPM (rizici ne provedbe mjere). Neke od mjera zahtijevaju dodatne materijale za provedbu na koje će dodatni opis mjere upućivati i koje je potrebno primijeniti kako bi se mjera provela u skladu s okvirom i osigurala zaštita na adekvatnoj razini. Ukoliko neka mjera preuzima u cjelosti ili djelomično naputke iz drugih okvira, u opisu je navedeno koji su to okviri odnosno smjernice okvira na kojima se mjera zasniva.

6.2 Pregled okvira

PODRUČJE	MJERA	DODATNE REFERENCE	MALA PODUZEĆA	SREDNJA PODUZEĆA
A	**A-1: Izrađen je popis uređaja (mobilnih uređaja, prijenosnih i stolnih računala, poslužitelja, usmjernika, preklopnika itd.) zajedno s informacijom o lokaciji uređaja** *Podatke za izradu popisa uređaja najlakše je dobiti od samih zaposlenika pitajući ih koje uređaje i u koje svrhe koriste*. ***Dodatak kao pomoć pri provedbi:*** *Prilog 1 - Tablica za popis uređaja* ***RNPM:*** *neprepoznavanje ulaznih i izlaznih vektora za kibernetičke napade*	**CIS Controls** 1 **NIST** ID.AM-1 **COBIT 5** BAI09.01, BAI09.02	X	X
A	**A-2: Izrađen je popis softvera uz poslovne funkcije za koje se koristi, zajedno s popisom korisnika tog softvera (uz imena i prezimena navesti i korisničke račune)** *Podatke za izradu popisa softvera najlakše je dobiti od samih zaposlenika pitajući ih koji softver i u koje svrhe koriste*. ***Dodatak kao pomoć pri provedbi:*** *Prilog 2 - Tablica za popis softvera* ***RNPM:*** *neprepoznavanje ulaznih i izlaznih vektora za kibernetičke napade*	**CIS Controls** 2 **NIST** ID.AM-2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05		X

A	**A-3: Koristi se adekvatan softver za pohranu korisničkih računa i pristupnih podataka s mogućnošću podsjetnika za periodičnu promjenu zaporka** *Ovi se podaci mogu dobiti prilikom provedbe mjere A-2 istovremeno upisujući pristupne podatke u neki od softvera za pohranu zaporka s kriptografskom zaštitom. Neki od primjera takvih softvera su: Dashlane, LastPass, Passwork i Kaspersky Password Manager.* ***RNPM:** nemogućnost pristupa prilikom i oporavka računa nakon napada*	**NIST** PR.AC-1 **CIS Controls** 4, 16 **COBIT 5** DSS05.04, DSS06.03	X	X
A	**A-4: Određene su osobe koje će provoditi redovno održavanje adekvatne razine kibernetičke sigurnosti i pohađati primjerene edukacije** *U malim poduzećima to su često samo vlasnici i na njima je ili da unajme vanjske konzultante ili da sami provode održavanje adekvatne razine kibernetičke sigurnosti. U srednjim poduzećima to će najčešće biti jedan od informatičara, s time da je potrebna periodična edukacija (praćenje internetskih portala, sigurnosnih izvještaja (npr. Kaspersky Lab Global IT Risk Report), webinari i slično).* ***RNPM:** neadekvatno znanje zaduženih osoba o razini kibernetičke sigurnosti poduzeća*	**NIST** ID.GV-2 **CIS Controls** 17 **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04		X
A	**A-5: Izrađen je popis trećih strana (poslovnih partnera, dobavljača roba i usluga, pružatelja telekomunikacijskih usluga i sličnih) koje sudjeluju u razmjeni digitalnih podataka s poduzećem s navedenim kategorijama podataka koje se razmjenjuju** *Ovim popisom srednja poduzeća dobivaju širu sliku o tome koji podaci ulaze i izlaze iz informacijskog sustava poduzeća te mogu identificirati one kanale koji zahtijevaju dodatnu kriptografsku ili drugu vrstu zaštite* ***Dodatak kao pomoć pri provedbi:*** *Prilog 3 - Tablica za popis podataka u razmjeni s trećim stranama* ***RNPM:** nemogućnost identifikacije ulaznih vektora za kibernetičke napade*	**NIST** ID.BE-2 **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05		X

A	**A-6: Izrađen je dokument koji propisuje minimalnu sigurnosnu razinu mreža koje se koriste u poslovanju (LAN, VPN i drugih)** *Ovdje se prvenstveno radi o propisivanju protokola minimalne zaštite mreža za podatke u prijenosu (značajke HTTPS, SFTP i drugih protokola).*	**NIST** ID.BE-5 **COBIT 5** BAI03.02, DSS04.02		X
A	**A-7: Izrađen je popis ključnog hardvera i softvera bez kojih poduzeće ne bi moglo poslovati ili bi poslovalo s gubitkom performansi** *Kritični softver je za mala poduzeća najčešće računovodstveni softver i softver za prodaju (POS softver i slično), dok za srednja poduzeća treba uzeti u obzir i softver za skladištenje, logistiku, upravljanje ljudskim potencijalima, softver za obradu dokumenata i slične.* ***Dodatak kao pomoć pri provedbi:*** *Prilog 4 - Tablica za popis ključnog hardvera i softvera* ***RNPM:** nemogućnost identifikacije ulaznih vektora za kibernetičke napade kritične infrastrukture*	**NIST** ID.BE-4 **COBIT 5** BAI03.02, DSS04.02	X	X
A	**A-8: Razvijena je politika kibernetičke sigurnosti uz raspored provjere razine kibernetičke sigurnosti i popisane su odgovorne osobe koje će provesti provjeru i na koji način** *Jednostavnije politike kibernetičke sigurnosti mogu se pregledati na sljedećim poveznicama:* ● *https://www.talentlyft.com/en/resources/cyber-security-policy [pristupano datuma 1.9.2019.]* ● *https://resources.workable.com/cyber-security-policy [pristupano datuma 1.9.2019.]* *Nešto opsežnije politike kibernetičke sigurnosti mogu se pregledati na sljedećim poveznicama:* ● *https://www.sans.org/security-resources/policies [pristupano datuma 1.9.2019.]* ● *https://link.springer.com/chapter/10.1007/978-1-4302-6083-7_19 [pristupano datuma 1.9.2019.]*	**CIS Controls** 17, 18, 19, 20 **NIST** ID.GV-1 **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02		X

A	**A-9: Popisani su zakoni, okviri i standardi s kojima poduzeće mora u sklopu poslovanja biti sukladno** *Zakonski, okviri i standardi s kojima poduzeće prema Zakonu treba biti sukladno često postavljaju barem minimalnu razinu kibernetičke zaštite informacijskog sustava poduzeća.*		X	X
A	**A-10: Razvijena je politika edukacije zaposlenika o kibernetičkoj sigurnosti** *Potrebno je odrediti koja će se osoba na koji način, o kojim temama i u kojem periodu educirati o kibernetičkoj sigurnosti.* ***RNPM:** loša educiranost o mogućim prijetnjama informacijskom sustavu poduzeća*	**NIST** PR.AT **CIS Controls** 17 **COBIT 5** APO01.02, APO07.02, APO07.03, APO07.06, APO10.04, BAI05.07, DSS05.04, DSS06.03, EDM01.01	X	X
A	**A-11: Razvijena je politika ažuriranja softvera i odgovorne osobe koje će je provoditi** *Zakrpe u softverima omogućavaju adekvatnu zaštitu od aktualnih kibernetičkih prijetnji, stoga je potrebno odrediti koje osobe su odgovorne za ažuriranje kojeg softvera.* ***RNPM:** nedovoljna zaštita softvera koji služi kao potpora poslovanju, novi vektori za kibernetičke napade*	**CIS Controls** 2	X	X
A	**A-12: Identificirane su ključne prijetnje hardverskoj i softverskoj infrastrukturi** *Neki od primjera ključnih prijetnji: Trojans, Worms, CryptoLockers, DDoS, Network Intrusion* ***RNPM:** nemogućnost zaštite od prijetnji s najvišim rizikom pojave*	**NIST** ID.RA-1, ID.RA-3 **CIS Controls** 20 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04	X	X

A	**A-13: Propisati standarde za prijenos podataka u sklopu lanca vrijednosti (kroz ugovore s dobavljačima, ugovore s kupcima i druge)** *Ugovori s partnerima moraju sadržavati odrednice o načinima komunikacije (koje su ključne osobe za komunikaciju i razmjenu kojih vrsta podataka) i minimalnom zaštitom podataka u prijenosu (primjerice zaštita .zip datoteka enkripcijom, minimalna zaštita putem SFTP-a, SSL/TLS-a i slično)* ***RNPM:** dodatni ulazni vektori za kibernetičke napade; povećani rizik od krađe podataka*	**NIST** ID.SC-2, PR.DS-2 **CIS Controls** 13, 14 **COBIT 5** APO01.06, APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03, DSS05.02, DSS06.06		X
A	**A-14: Popisani su najvažniji skupovi podataka (e-mail pretinci, arhive, baze podataka i slično) i za njih mjere zaštite i arhiviranja te odgovorne osobe** ***Dodatak kao pomoć pri provedbi:*** *Prilog 5 - Tablica za popis najvažnijih skupova podataka* ***RNPM:** povećani rizik od gubitka ključnih podataka za poslovanje poduzeća*	**NIST** PR.IP-4, PR.DS-2 **CIS Controls** 10, 13, 14 **COBIT 5** APO01.06, APO13.01, BAI02.01, BAI06.01, DSS01.01, DSS04.07, DSS05.03, DSS06.06, DSS04.07	X	X
A	**A-15: Propisani su standardi za protokole razmjene podataka u prometu koji će se implementirati unutar internog informacijskog sustava** *Propisati minimalne zahtjeve za sigurnost protokola za podatke u prijenosu (HTTPS, SFTP i slični) unutar politike kibernetičke sigurnosti iz mjere A-8.* ***RNPM:** povećani rizik od krađe podataka*	**NIST** PR.DS-2 **CIS Controls** 13 **COBIT 5** APO01.06, DSS05.02, DSS06.06		X

A	**A-16: Uključena je opcija vođenja radnih zapisa (engl. *audit logs*) u ključnim softverima** *Većina softvera ima mogućnost vođenja radnih zapisa, a za one koji nemaju potrebno je provjeriti mogućnost implementacije podsustava za vođenje radnih zapisa.* ***RNPM:** nemogućnost identifikacije izvora i načina nastanka prijetnje kako bi se provela zaštita od sličnih prijetnji*	**NIST** PR.PT-1 **CIS Controls** 6 **COBIT 5** DSS05.04		X
A	**A-17: Izrađeni su procesi odgovora na incidente i oporavka od incidenata** *Najjednostavniji način je objediniti odluke o odgovorima na incidente i oporavku od incidenata unutar politike kibernetičke sigurnosti iz mjere A-8.* ***RNPM:** povećani rizik da će zaposlenici prilikom napada i oporavka donositi štetne odluke za poduzeće*	**NIST** ID.RA-6 **CIS Controls** 19 **COBIT 5** APO12.05, APO13.02	X	X
B	**B-1: Uspostavljeno je redovno upravljanje korisničkim računima (upravljanje pristupom, upravljanje ulogama i ovlastima, promjena zaporka, upravljanje jedinstvenošću i jakosti zaporka)** *Za ovu mjeru djelomično se koristi i softver za upravljanje zaporkama iz mjere A-3, dok je za upravljanje ulogama i pristupom potrebno periodično provjeriti svaki softver (prvenstveno kritični softver) sa izrađenih popisa iz mjera A-2 i A-7. Dijeljenje zaporka prema krajnjim korisnicima računa potrebno je obaviti sigurnim komunikacijskim kanalom sukladno mjeri A-15.* ***RNPM:** zastarjele i slabe zaporke stvaraju povećani rizik od neovlaštenog pristupa informacijskom sustavu poduzeća*	**NIST** PR.AC-1 **CIS Controls** 4 **COBIT 5** DSS05.04, DSS06.03	X	X

B	**B-2: Uspostavljene su dvofaktorske prijave u svakom sustavu gdje je to moguće i koriste se *anti-bruteforce* zaštite** *Dvofaktorske prijave (najčešće SMS-om ili e-poštom) danas su široko dostupna opcija i nužne su za kritični softver s popisa iz mjere A-7 koji sadrži kritične skupove podataka s popisa iz mjere A-14, a koji nisu dio operativne funkcije poduzeća (primjerice prijava na POS softver na prodajnom mjestu). Anti-bruteforce zaštita potrebna je u svakom softveru s popisa iz mjere A-2 i danas predstavlja minimalan zahtjev sigurnosti.* ***RNPM:** povećani rizik od neovlaštenog pristupa*	**NIST** PR.AC-7 **CIS Controls** 4	X	X
B	**B-3: Kritični skupovi podataka fizički su i tehnički zaštićeni** ***RNPM:** povećani rizik od curenja i gubitka podataka*	**NIST** PR.DS-1, PR.DS-3, PR.DS-5 **CIS Controls** 13 **COBIT 5** APO01.06, BAI02.01, BAI06.01, BAI09.03, DSS04.07, DSS05.03, DSS05.04, DSS05.07, DSS06.02, DSS06.06	X	X
B	**B-4: Pristup podacima informacijskog sustava ograničen je na *need-to-know* principu** *Need-to-know princip predstavlja princip dodjele pristupa prema kojem osoba treba imati pristup samo do one razine koja joj je potrebna za obavljanje dodijeljenih poslova. U praksi se često administratorski računi daju većem broju zaposlenika kako bi se "olakšalo" pristupanje sustavu, što dovodi poduzeće u rizik od curenja informacija izvan poduzeća od strane zaposlenika niže razine. Kako zaposlenici niže razine često ne pridodaju dovoljno pažnje zaštiti pristupnih podataka, povećan je i rizik od neovlaštenog pristupa* ***RNPM:** povećani rizik od curenja informacija, povećani rizik od neovlaštenog pristupa*	**NIST** PR.AC-4 **CIS Controls** 14 **COBIT 5** DSS05.04		X

B	**B-5: Sve propisane mjere zaštite iz područja A sukladne su sa standardima industrije i zadovoljavaju minimalne tehničke uvjete** *Potrebno se savjetovati sa stručnjacima iz industrije u kojoj poduzeće posluje kako bi se saznale poslovne prakse i slučajevi iz svakodevnog poslovanja.*	**NIST** ID.BE-2	X	X
B	**B-6: Korisnici ključnih informacijskih sustava educirani su i spremni na odgovore na aktualne prijetnje i rizike** ***RNPM:*** *neadekvatno ponašanje zaposlenika prilikom uočavanja incidenta*	**NIST** PR.AT **CIS Controls** 17 **COBIT 5** APO01.02, APO07.02, APO07.03, APO07.06, APO10.04, BAI05.07, DSS05.04, DSS06.03, EDM01.01		X
B	**B-7: Uprava poduzeća razumije tko, kada i na koji način ima pristup kojem dijelu informacijskog sustava** ***RNPM:*** *uprava nema saznanja kome se i na koji način obratiti prilikom odvijanja incidenta ili prilikom oporavka*	**NIST** ID.AM-6 **CIS Controls** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03	X	X

B	**B-8: Politika kibernetičke sigurnosti propisana je od strane uprave i osobe koje su zadužene za njenu provedbu su adekvatno educirane i s njom u potpunosti upoznate** *Prema razvijenoj politici kibernetičke sigurnosti iz mjere A-8, potrebno je dobiti odobrenje uprave i uprava mora propisati politiku kao važeću, a zadužene osobe moraju je iskomunicirati ostatku organizacije.* ***RNPM:** uprava ne razumije ulogu kibernetičke sigurnosti u poduzeću, zadužene osobe nisu sigurne kako postupati prilikom uočavanja događaja i incidenata ili prilikom oporavka*	**NIST** PR.AT, ID.GV-1 **CIS Controls** 17, 19 **COBIT 5** APO01.02, APO01.03, APO07.02, APO07.03, APO07.06, APO10.04, APO13.01, BAI05.07, DSS05.04, DSS06.03, EDM01.01, EDM01.02		X
B	**B-9: Podaci u mirovanju i prijenosu su adekvatno fizički i softverski zaštićeni** *Podaci u prijenosu moraju se štititi sukladno standardima iz mjere A-15, dok se kritični skupovi podataka moraju štititi sukladno mjeri A-14.* ***RNPM:** rizik od gubitka i curenja informacija*	**NIST** PR.DS-1, PR.DS-2 **CIS Controls** 13, 14 **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.02, DSS05.03, DSS06.06	X	X
B	**B-10: Postoji periodično stvaranje sigurnosnih kopija kritičnih skupova podataka** *Periodično stvaranje sigurnosnih kopija mora se odvijati prema politici kibernetičke sigurnosti iz mjere A-8 za skupove s popisa iz mjere A-14.* ***RNPM:** rizik od gubitka podataka (primjerice prilikom napada CryptoLockerom)*	**NIST** PR.IP-4 **CIS Controls** 10 **COBIT 5** APO13.01, DSS01.01, DSS04.07	X	X

B	**B-11: Radni zapisi (engl. *audit logs*) se redovno pregledavaju i arhiviraju** ***RNPM:*** *nemogućnost identifikacije izvora i načina nastanka prijetnje kako bi se provela zaštita od sličnih prijetnji*	**NIST** PR.PT-1 **CIS Controls** 6.2, 8.8, 14.9 **COBIT 5** DSS05.04		X
B	**B-12: Softver se redovno ažurira prema propisanoj politici ažuriranja softvera** *Provjeriti mogućnost automatiziranog ažuriranja s uključenim obavijestima o provedenim ažuriranjima.* ***RNPM:*** *nedovoljna zaštita softvera koji služi kao potpora poslovanju, novi vektori za kibernetičke napade*	**CIS Controls** 2.2, 3.4, 3.5, 8.2, 11.4	X	X
B	**B-13: Odgovorne osobe periodično provjeravaju razinu kibernetičke sigurnosti na propisani način, izvještavajući upravu o uočenim nepravilnostima i prostorima za poboljšanja** *Za periodičnu provjeru koristi se politika kibernetičke sigurnosti iz mjere A-8, a provjeru i izvještavanje provode određene osobe za provjeru razine kibernetičke sigurnosti iz mjere A-4.* ***RNPM:*** *uprava nema saznanja o razini kibernetičke sigurnosti poduzeća*	**CIS Controls** 17, 19 **NIST** ID.GV-1 **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02	X	X
B	**B-14: Podaci se na siguran način uništavaju** *Datoteke koje stavimo u "smeće" mogu se u kraćem periodu vratiti. Potrebno je koristiti adekvatni softver za sigurno uništavanje (primjerice Kaspersky File Shredder, Eraser, Securely File Shredder i slični).* ***RNPM:*** *napadači prilikom neovlaštenog pristupa imaju dodatnu priliku vratiti datoteke koje su trebale biti uništene*	**NIST** PR.IP-6 **COBIT 5** BAI09.03, DSS05.06	X	X

B	**B-15: Odjel upravljanja ljudskim resursima usklađen je s odgovornim osobama za provedbu održavanja adekvatne razine kibernetičke sigurnosti** *Odjel upravljanja ljudskih resursa trebao bi poznavati i periodično mjeriti kompetencije osoba zaduženih za područje kibernetičke sigurnosti. Također, u srednjim poduzećima odjel ljudskih resursa često ima ulogu objavljivanja kritičnih obavijesti zaposlenicima, pa može poslužiti za istu svrhu prilikom detekcije, odvijanja incidenata i oporavka.* ***RNPM:** povećani rizik od neadekvatnog znanja o kibernetičkoj sigurnosti*	**NIST** PR.AT-5, PR.IP-11 **CIS Controls** 17 **COBIT 5** APO07.03		X
B	**B-16: Redovno se provodi procjena prijetnji i rizika informacijskom sustavu poduzeća** Procjena prijetnji i rizika treba se provoditi sukladno politici kibernetičke sigurnosti iz mjere A-8. **RNPM:** ne mogućnost identifikacije najrizičnijih dijelova informacijskog sustava poduzeća	**NIST** ID.RA **CIS Controls** 3 **COBIT 5** APO12, APO12, APO12, APO12, DSS04.02, DSS05, DSS05		X
B	**B-17: Treće strane u sklopu lanca vrijednosti upoznate su i sukladne propisanim standardima iz mjere A-3** *Potrebno je zatražiti potvrdu trećih strana da zaista razumiju potpisane ugovore i provjeriti koriste li se propisani standardi.* ***RNPM:** dodatni ulazni vektori za kibernetičke napade, povećani rizik od krađe podataka*	**NIST** ID.BE-2 **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05		X

B	**B-18: Poslužiteljska infrastruktura pod redovnim je nadzorom stručnjaka** *Poslužiteljska infrastruktura predstavlja kritičnu infrastrukturu za digitalno transformirana poduzeća. Za mala poduzeća gotovo najlakši način za održavanje poslužitelja je plaćanje održavanja hosting poduzeću koje pruža usluge najma poslužitelja, dok će za srednja poduzeća to često obavljati i sami informatičari koji ujedno i provode kibernetičku sigurnost, no tada u obzir treba uzeti i adekvatnu edukaciju i kompetencije.* ***RNPM:** neadekvatna zaštita kritične infrastrukture*	**CIS Controls** 5	X	X
B	**B-19: Izvorni kôd ključnih informacijskih sustava redovno se provjerava, ažurira i usklađuje sa standardima industrije** *Preporuča se korištenje alata za provjeru sigurnosti izvornog kôda, ali i periodična ručna provjera izvornog kôda informacijskih sustava.* ***RNPM:** sigurnosni propusti informacijske infrastrukture poduzeća*	**NIST** PR.DS-6 **CIS Controls** 18 **COBIT 5** APO01.06, BAI06.01, DSS06.02		X
B	**B-20: Korisnički računi izrađeni su i dodijeljeni na način da je osigurana mogućnost utvrđivanja odgovornosti (preporuča se jedan korisnički račun po osobi)** *Nerijetki slučajevi iz prakse pokazuju da se u malim i srednjim poduzećima korisnički računi dijele između više korisnika, što korisnicima omogućava izbjegavanje odgovornosti pod izlikom da je tada "lakše" korištenje sustava jer ne moraju pamtiti dodatna imena i zaporke. Najpoželjniji način dodjele korisničkih računa je 1-1 način, dakle jedna osoba dobiva jedan korisnički račun (otvoren na ime i prezime) sa jedinstvenom zaporkom (koristiti softver iz mjere A-3).* ***RNPM:** nemogućnost utvrđivanja odgovornosti pri analizi incidenata*	**NIST** DE.DP-1 **CIS Controls** 16	X	X

B	**B-21: Svi zaposlenici (koji su sudionici informacijskog sustava) dobro su upoznati s procesima oporavka od incidenata** *Nije dovoljno samo izraditi procese oporavka od incidenata iz mjere A-17, već je potrebno i utvrditi jesu li zaposlenici zaista dobro upoznati s procesima.* ***RNPM:** povećani rizik da će zaposlenici prilikom napada i oporavka donositi štetne odluke za poduzeće*	**NIST** PR.AT-1 **CIS Controls** 17, 19 **COBIT 5** APO07.03, BAI05.07		X
B	**B-22: Periodično se provode penetracijski testovi** ***RNPM:** nemogućnost identifikacije i detekcije budućih prijetnji informacijskom sustavu poduzeća*	**CIS Controls** 20		X
C	**C-1: Uočeni kritični događaji su popisani** ***Dodatak kao pomoć pri provedbi:*** *Prilog 6 - Tablica za popis uočenih događaja* **RNPM:** nemogućnost praćenja uočenih događaja u svrhu predviđanja budućih prijetnji i analize utjecaja na ostatak informacijskog sustava poduzeća	**CIS Controls** 19.1	X	X
C	**C-2: Uočeni događaji analiziraju se u svrhu predviđanja budućih prijetnji** *Koristiti se popisom iz mjere C-1.* ***RNPM:** nemogućnost postavljanja preventivnih mjera za buduće prijetnje*	**NIST** DE.AE-2, DE.CM-3 **COBIT 5** DSS05.07		X

C	**C-3: Uočeni događaji analiziraju se u svrhu otkrivanja utjecaja na ostatak informacijskog sustava poduzeća** *Koristiti se popisom iz mjere C-1.* ***RNPM:*** *nemogućnost otkrivanja utjecaja događaja na ostatak informacijskog sustava poduzeća*	**NIST** DE.AE-4 **COBIT 5** APO12.06, DSS03.01	X	X
C	**C-4: Redovno se rade duboka skeniranja pomoću antivirusnog softvera** ***RNPM:*** *nemogućnost uočavanja kritičnih prijetnji informacijskom sustavu poduzeća i reagiranje odgovorima na iste*	**NIST** DE.CM-8 **CIS Controls** 3 **COBIT 5** BAI03.10, DSS05.01	X	X
C	**C-5: Redovno se provodi skeniranje mobilnih uređaja antivirusnim softverom** ***RNPM:*** *nemogućnost uočavanja kritičnih prijetnji informacijskom sustavu poduzeća i reagiranje odgovorima na iste*	**NIST** DE.CM-8 **CIS Controls** 3 **COBIT 5** BAI03.10, DSS05.01	X	X
C	**C-6: Uspostavljeni su mehanizmi otkrivanja događaja u ključnim informacijskim sustavima** *Korištenje automatiziranih mehanizama za otkrivanje događaja (kao što su radni zapisi (engl. audit logs), automatizirane trenutne obavijesti o uočenim događajima u sustavu, automatizirane obavijesti SMS-om ili e-poštom prilikom sumnjive prijave u sustav, zaštita od krađe i slično).* ***RNPM:*** *nemogućnost uočavanja kritičnih prijetnji informacijskom sustavu poduzeća i reagiranje odgovorima na iste*	**NIST** DE.CM-1, DE.CM-2 CIS Controls 3	X	X
C	**C-7: Mehanizmi otkrivanja događaja redovno se testiraju i unapređuju** ***RNPM:*** *nemogućnost otkrivanja novih, sofisticiranijih vrsta prijetnji*	**NIST** DE.DP-5 **COBIT 5** APO11.06, APO12.06, DSS04.05	X	X

D	**D-1: Incidenti su popisani** ***Dodatak kao pomoć pri provedbi:*** *Prilog 7 - Tablica za popis incidenata*	**NIST** RS.MI **COBIT 5** APO12.06	X	X
D	**D-2: Incidenti se rješavaju u skladu sa standardima industrije i od strane stručnjaka** *Vanjski stručnjaci ili poduzeća za kibernetičku sigurnost ovdje su od kritične važnosti kako bi se incidenti uklonili i kako bi se proveo adekvatan oporavak od incidenata.* ***RNPM:** povećani rizik da je incident uklonjen, ali prijetnja nije uklonjena*	**NIST** RS.MI **COBIT 5** APO12.06	X	X
D	**D-3: Svi zaposlenici (koji su sudionici informacijskog sustava) tokom odvijanja incidenata postupaju sukladno propisanim pravilima i edukacijama**	**NIST** DE.AE-5, RS.CO-1 **CIS Controls** 19.2		X
D	**D-4: Informacije o incidentima jasno se prenose putem definiranog komunikacijskog kanala koji osigurava brzo davanje informacije s mogućnošću pregleda povijesti razgovora** *Kao jednostavniji komunikacijski kanal može se koristiti SMS, no preporuča se interni sustav za komunikaciju, kao što su to Slack, Asana, Bitrix24, Zoho Cliq i slični. Komunikacija putem telefonskog razgovora ne ostavlja trajne zapise o tome tko je (ili nije) kada i koju informaciju prenio.* ***RNPM:** nemogućnost utvrđivanja tko je informiran o incidentu i koje su informacije prenijete*	**NIST** RS.CO-2, RS.CO-3 **CIS Controls** 19.2, 19.3 **COBIT 5** EDM03.02, APO01.02, APO12.03, DSS01.03		X
D	**D-5: Postoji komunikacija s upravom prilikom odvijanja incidenta** *Voditi se načelima iz mjere D-4.* ***RNPM:** nemogućnost utvrđivanja tko je informiran o incidentu i koje su informacije prenijete*	**NIST** RS.CO-4 **COBIT 5** DSS03.04	X	X

D	**D-6: Radi se računalna forenzika** ***RNPM:*** *nemogućnost identifikacije osobe koja je počinila napad, nemogućnost utvrđivanja dokaza na sudu*	**NIST** RS.AN-4 **COBIT 5** DSS02.02		X
D	**D-7: Incidenti se u karanteni analiziraju za procjenu dodatne štete ostatku informacijskog sustava** ***RNPM:*** *nakon što je incident uklonjen, postoji povećani rizik da su prijetnje i dalje aktivne u ostatku informacijskog sustava*	**NIST** RS.AN-2 **CIS Controls** 19.8 **COBIT 5** DSS02.02		X
E	**E-1: Procesi oporavka od incidenata poštuju se pri oporavku od incidenata** *Prema propisanoj politici kibernetičke sigurnosti iz mjere A-8.*	**NIST** RC.RP-1 **CIS Controls** 10 **COBIT 5** APO12.06, DSS02.05, DSS03.04	X	X
E	**E-2: Procesi oporavka se redovno ažuriraju i unapređuju** *Napadi s vremenom postaju sve sofisticiraniji i donose veću štetu u kraćem roku, zbog čega je potrebno provjeravati, ažurirati i unapređivati procese oporavka.*	**NIST** RC.IM-1, RC.IM-2 **CIS Controls** 10 **COBIT 5** APO12.06, BAI05.07, BAI07.08, DSS04.08	X	X
E	**E-3: Nakon incidenta analiziraju se dijelovi informacijskih sustava za dodatne (kolateralne) štete i takve štete se saniraju** ***RNPM:*** *nakon što je incident uklonjen, postoji mogućnost da nije uklonjena i sva šteta*	**CIS Controls** 19	X	X
E	**E-4: Uprava je pravovremeno obaviještena o oporavku i načinima sanacije šteta** *Prema propisanoj politici kibernetičke sigurnosti iz mjere A-8.* ***RNPM:*** *uprava nema saznanja o tome kako je incident riješen i na koji je način sanirana šteta*	**NIST** RC.CO-3 **COBIT 5** APO12.06	X	X

E	**E-5: Svaki incident zajedno s opisom načinjene štete se ocjenjuje, kao i uspješnost oporavka i saniranja štete** *Koristiti tablicu za popis incidenata iz mjere D-1.* ***RNPM:*** *nemogućnost utvrđivanja koji su incidenti imali najveći utjecaj na informacijski sustav poduzeća*	**CIS Controls** 19		X

Tablica 1, Pregled okvira

6.3 Pripreme za provedbu okvira

Važno je napomenuti da cilj CFSMB-a nije usporavanje ili na bilo koji način onemogućavanje poslovanja poduzeća. Svaka od mjera treba se ili prilagoditi trenutnoj situaciji poduzeća (ako bi prilagodba rezultirala dovoljnom razinom kibernetičke sigurnosti s kojom se uprava slaže) ili je potrebno uvesti i koristiti druge tehnologije koje su sukladne toj mjeri, a sve to bez usporavanja ili onemogućavanja poslovanja poduzeća.

6.3.1 Mala poduzeća

U malim poduzećima često sami vlasnici provode zadatke osiguravanja adekvatne kibernetičke sigurnosti. S tom pretpostavkom, vlasnik poduzeća je taj koji mora biti upoznat s CSFMB-om. Nije nužno, no preporučljivo je upoznavanje s *CIS Controls* okvirom radi boljeg razumijevanja koje su mjere bitne za poduzeće, a koje je potrebno u neku ruku modificirati. Vlasnik sam najbolje razumije opseg informacijskih tehnologija u vlastitom poduzeću, no svakako se preporuča savjetovanje sa stručnjakom za kibernetičku sigurnost ili revizorom informacijskih sustava tokom pripreme, provedbe i održavanja sukladnosti s CFSMB-om.

6.3.2 Srednja poduzeća

U srednjim poduzećima najčešće postoji barem jedna osoba u ulozi informatičara. Ta osoba mora se detaljno upoznati s CFSMB-om i razumjeti kontekst poduzeća u ekonomskom okruženju kako bi upravi mogla predstaviti CFSMB i način provedbe sukladnosti. Preporuča se i čitanje povezanih okvira: NIST, *CIS Controls* i COBIT 5. Važno je detaljno poznavanje *CIS Controls* i dobro poznavanje NIST okvira, dok COBIT 5 služi kao nit vodilja radi šireg razumijevanja na koji način odjel informatike korelira s upravom u provođenju kibernetičke sigurnosti. Poželjno je i osnovno znanje korporativnog upravljanja informatikom i razumijevanje na koji način su informacijske tehnologije uključene na operativnoj, taktičkoj i strateškoj razini.

Prilikom stvaranja tima za provedbu sukladnosti s okvirom potrebno je provjeriti jesu li odabrane osobe kompetentne u području kibernetičke i informacijske sigurnosti, kao i njihovo općenito znanje o provedbi okvira za kibernetičku i informacijsku sigurnost. Te osobe ne moraju unaprijed biti upoznate s CFSMB-om (obzirom na njegovu pojednostavljenost u odnosu na druge okvire na kojima se temelji), već se s njim mogu upoznati i nakon procesa odluke tko će biti dio tima.

6.4 Metodologija provedbe okvira

Okvir je izrađen na način da se provodi područje po područje slijedeći abecedni redoslijed:

1. A - Identifikacija,
2. B - Zaštita,
3. C - Otkrivanje,
4. D - Odgovaranje i
5. E - Oporavak.

Uz svaku mjeru gdje je potrebno, priložene su tablice koje se nalaze u prilozima ovog rada, a koje olakšavaju provedbu mjera i praćenje i ocjenjivanje događaja, incidenata i oporavka. Preporuča se vođenje tablica istih struktura u softverima za obradu tablica kao što su to Microsoft Excel, OpenOffice ili LibreOffice s mogućnošću dijeljenja tablica između više osoba ukoliko više osoba istovremeno vodi tablice i treba imati mogućnost istovremenog ažuriranja i unosa podataka.

Svaki puta kada se provodi sukladnost s okvirom stvara se jedna *iteracija provedbe sukladnosti*. Ukoliko određena mjera zahtjeva radikalne promjene u poduzeću, predlaže se postepeno usklađivanje s mjerom kroz više iteracija provedbe sukladnosti s okvirom. Ukoliko poduzeće u određenoj iteraciji provedbe sukladnosti nije sukladno s nekom od mjera, potrebno je od uprave zatražiti odobrenje da provedba sukladnosti prođe bez odabranih mjera i da se sukladnost s tim mjerama provede u budućoj iteraciji.

Kod malih poduzeća, ukoliko osobe koje provode sukladnosti nisu vlasnici poduzeća, predlaže se redovita koordinacija s vlasnicima putem e-pošte (obzirom na manji obujam mjera koje je potrebno provesti) ili putem sastanaka.

U slučaju poduzeća srednje veličine, ukoliko osobe koje provode sukladnost s okvirom nisu istovremeno i članovi uprave, preporuča se da te osobe imaju redovitu komunikaciju s upravom u obliku tjednih/mjesečnih sastanaka gdje će se postaviti ciljevi koje će se mjere u kojim vremenskim rasponima provoditi, na koji način i koji će biti obuhvat tih mjera. Postoji mogućnost da neke mjere neće zahtijevati obuhvat cijelog poduzeća (ukoliko se neki odjeli ne koriste digitalnim tehnologijama, primjerice ako se radi o skladištu, tj. osobama koje rade isključivo fizički posao u skladištu). Od ključne važnosti je pismeno donošenje odluka, dakle

treba postojati jasan zapis kojim se potvrđuje koje akcije i mjere uprava poduzeća želi da tim za provođenje sukladnosti s okvirom provede.

6.5 Kontinuitet održavanja sukladnosti s okvirom

Jedna iteracija provedbe sukladnosti s okvirom svakako ne znači da je poduzeće i dalje sukladno s minimalnim zahtjevima kibernetičke sigurnosti današnjice. Potrebno je periodično (preporuča se tromjesečno za srednja poduzeća i dvogodišnje za mala poduzeća) provesti novu iteraciju sukladnosti s okvirom.

Kako bi se održao adekvatan kontinuitet održavanja sukladnosti s okvirom, preporuča se da se tim za provedbu sukladnosti mijenja prije početka iduće iteracije provedbe sukladnosti, ukoliko je promjena tima potrebna. Ukoliko nema potrebe za promjenom članova tima, moraju se osigurati edukacije članovima tima prije svake provedbe sukladnosti.

Određene mjere provode se kroz cijelo vrijeme poslovanja (kao što je to praćenje događaja, incidenata i slično) s preporukom da te mjere provode upravo članovi tima za provedbu sukladnosti između dviju iteracija provedbe sukladnosti.

8 Zaključak

Digitalna transformacija poduzeća stvorila je novo okruženje digitalne ekonomije, gdje je poslovanje poduzeća uvjetovano informacijskom infrastrukturom i njenim razvojem. Kako su razvoj informacijske infrastrukture i primjena digitalnih tehnologija u poslovanju postali jedni od temeljnih strateških ciljeva digitalno transformiranih poduzeća, otvoreni su novi vektori za napad unutar kibernetičkog prostora. Održavanje adekvatne razine kibernetičke sigurnosti ponajviše se oslanja na primjenu okvira za kibernetičku sigurnosti kao što su NIST, CIS *Controls*, PCI DSS, COBIT 5 i obitelj ISO 27K standarda. Postojeći okviri za kibernetičku sigurnost ponajviše se okreću javnim poduzećima i korporacijama, s time da mala i srednja poduzeća moraju skrojiti okvir na način da izbacuju van suvišne smjernice. Upravo iz tog razloga u ovom je radu predstavljen CFSMB, okvir za upravljanje kibernetičkom sigurnošću za mala i srednja poduzeća, koji kroz pet područja (identifikacija, zaštita, otkrivanje, odgovaranje i oporavak) daje mjere kojima poduzeće može održavati adekvatnu razinu kibernetičke sigurnosti u današnjem okruženju. Osim toga što je primijenjen malim i srednjim subjektima ekonomije, okvir je izrađen na hrvatskom jeziku s priloženim tablicama za provedbu mjera, što znatno olakšava provedbu sukladnosti s okvirom. U radu su ukratko objašnjene pripreme za provedbu sukladnosti s okvirom, metodologija provedbe i kontinuitet održavanja sukladnosti, što služi kao osnovna nit vodilja pri osnivanju tima i organizacije provedbe sukladnosti s okvirom.

9 Literatura

1. Bogati, J. (2008.) *Norme informacijske sigurnosti ISO/IEC 27K*, Praktični menadžment, Vol. II, br. 3, str. 112-117
2. Center for Internet Security (2019.) *CIS Controls* [PDF]. Dostupno na: https://www.cisecurity.org/controls/
3. Dimensional Research (2016.) *Trends in Security Framework Adoption* [PDF]. Dostupno na: https://www.tenable.com/whitepapers/trends-in-security-framework-adoption
4. European Union Agency for Cybersecurity (2016.) *NCSS Good Practice Guide* [online]. Dostupno na: https://www.enisa.europa.eu/publications/ncss-good-practice-guide
5. Federal Communications Commission (2012.) *Cyber Security Planning Guide* [online]. Dostupno na: https://www.fcc.gov/cyberplanner
6. Humpreys. E. (2016.) *Implementing the ISO/IEC 27001 ISMS Standard*, Second Edition, Artech House, Norwood
7. ISACA (2013.) *COBIT 5 Enabling information* [online]. Dostupno na: http://www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Information-product- page.aspx
8. ISACA (2012.) *COBIT 5 Enabling Processes* [online]. Dostupno na: http://www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Processes-product-page.aspx
9. ISACA (2012.) *COBIT 5 Framework* [online]. Dostupno na: http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx
10. ISACA (Information Systems Audit and Control Association), *Glossary* [online]. Dostupno na: https://www.isaca.org/Pages/Glossary.aspx
11. ISACA (2012.) *COBIT 5 Implementation* [online]. Dostupno na: http://www.isaca.org/COBIT/Pages/COBIT-5-Implementation-product-page.aspx
12. ISO/IEC (2005.) *Information technology — Security techniques — Information security management systems — Requirements ISO/IEC 27001:2005(E)*, Switzerland
13. National Institute of Standards and Technology (2018.) *Framework for Improving Critical Infrastructure Cybersecurity* [PDF]. Dostupno na: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
14. National Institute of Standards and Technology (2016.) *Small Business Information Security: The Fundamentals* [online]. Dostupno na: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

15. NIST (National Institute of Standards and Technology), U.S. Department of Commerce, *CSRC (Computer Security Resource Center)* [online]. Dostupno na: https://csrc.nist.gov/Glossary
16. OWASP Foundation (2008.) *OWASP Testing Guide* [online]. Dostupno na: https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf
17. Panian, Ž. (2001.) *Kontrola i revizija informacijskih sustava*, Sinergija-nakladništvo d.o.o., Zagreb
18. Panian, Ž., Spremić, M. (2007.) *Korporativno upravljanje i revizija informacijskih sustava*, Zgombić & Partneri – nakladništvo i informatika d.o.o., Zagreb
19. PCI Security Standards Council, LLC (2018.) *Payment Card Industry (PCI) Data Security Standard* [PDF]. Dostupno na: https://www.pcisecuritystandards.org/document_library?document=pci_dss
20. Sifma.org (2017.) *Small Firms Cybersecurity Guidance* [online]. Dostupno na: https://www.sifma.org/wp-content/uploads/2017/07/small-firms-cybersecurity-guide-2017.pdf
21. Senft, S., Manson, D.P., Gonzales, C., Gallegos, F. (2004.) Information Technology Control and Audit (2nd Ed.), Auerbach Publications, CRC Press LLC, 2000 N.W. Corporate Blvd., Boca Raton, Florida 33431
22. Spremić, M. (2017.) *Digitalna transformacija poslovanja*, Sveučilišna tiskara d.o.o., Zagreb
23. Spremić, M. (2017.) *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije*, Sveučilišna tiskara d.o.o., Zagreb
24. The SysSec Consortium (2013.) *The Red Book* [online]. Dostupno na: http://www.red-book.eu/
25. Zavod za sigurnost informacijskih sustava (2015.) *The National Cyber Security Strategy of the Republic of Croatia* [online]. Dostupno na: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/croatian-cyber-security-strategy

10 Popis tablica

11 Popis slika

12 Prilozi

12.1 Prilog 1 - Tablica za popis uređaja

[A-1] Popis uređaja

Identifikacijska oznaka*	Puni naziv uređaja	Specifikacije uređaja**	Poveznica na detaljne specifikacije uređaja***	Lokacija uređaja****	Poslovne funkcije i namjene*****	Jamstvo vrijedi do datuma

* predlaže se dodjeljivanje identifikacijskih oznaka, pri čemu se na sami uređaj stavlja mala naljepnica s oznakom ukoliko je to moguće; primjer identifikacijske oznake: 0001, 0002, 0003 itd.

** primjer za stolno računalo: AMD Athlon 200GE up to 3.2GHz, 4GB DDR4, 120GB SSD, AMD Radeon Vega 3 Graphics, DVD-RW

*** staviti poveznicu na web stranicu koja prikazuje specifikacije uređaja

**** primjer: vanjsko poduzeće “Hosting XY”, odjel za informatiku, odjel za računovodstvo i knjigovodstvo

***** primjer: tablet za terenski rad, stolno računalo za rad u uredu, prijenosno računalo za rad od kuće

Izradio/la: _____ datuma ____.____._____.

12.2 Prilog 2 - Tablica za popis softvera

[A-2] Popis softvera

Identifikacijska oznaka*	Puni naziv softvera	Poslovne funkcije i namjene**	Aktivni korisnici (ime, prezime i korisnički račun)***	Poveznica na detaljne specifikacije softvera****	Softver održava*****	U vlasništvu ili u najmu

* predlaže se dodjeljivanje identifikacijskih oznaka; primjer identifikacijske oznake: 0001, 0002, 0003 itd.

** primjer: obrada računovodstvenih dokumenata, vođenje skladišta, upravljanje e-poštom

*** primjer: Janko Janković [jankojankovic]

**** staviti poveznicu na web stranicu koja prikazuje specifikacije softvera (minimalni zahtjevi i slično)

***** primjer: vanjsko poduzeće “Informatika XY”, vlastiti informatičar (primjerice za Microsoft Office 2016, održavatelj je “Microsoft”)

Izradio/la: _____ datuma ____.____._____.

12.3 Prilog 3 - Tablica za popis podataka u razmjeni s trećim stranama

[A-5] Podaci u razmjeni s trećim stranama

Puni naziv poduzeća	Poslovni kontekst*	Ključna kontakt osoba	Kategorije podataka u razmjeni**

* primjer: poslovni partner, dobavljač robe, dobavljač usluga, ispunjenje zakonodavnih obveza

** primjer: podaci o proizvodima, podaci o ljudskim potencijalima, podaci o klijentima

Izradio/la: _____ datuma ____.____._____.

12.4 Prilog 4 - Tablica za popis ključnog hardvera i softvera

[A-7] Popis ključnog hardvera i softvera

Identifikacijska oznaka hardvera/softvera*	A - Procijenjeni rizik od kibernetičkog napada**	B - Procijenjeni nivo kibernetičke zaštite***	C - Ukupna ocjena kibernetičke sigurnosti (što je manja, to hardver/softver zahtjeva veću pozornost)

* iz popisa za mjere A-1 i A-2

** procjena rizika od 1 do 10

*** procijenjeni nivo od 1 do 10

**** C = B - A

Izradio/la: _____ datuma ____.____._____.

12.5 Prilog 5 - Tablica za popis najvažnijih skupova podataka

[A-14] Popis najvažnijih skupova podataka

Dodijeljeni naziv podataka*	A - Procijenjeni rizik od kibernetičkog napada**	B - Procijenjeni nivo kibernetičke zaštite***	C - Ukupna ocjena kibernetičke sigurnosti (što je manja, to skupa podataka zahtjeva veću pozornost)	Mjere kibernetičke zaštite	Odgovorna osoba

* primjer: podaci o proizvodima, arhiva računovodstvenih i knjigovodstvenih dokumenata

** procjena rizika od 1 do 10

*** procijenjeni nivo od 1 do 10

**** C = B - A

Izradio/la: _____ datuma ____.____._____.

12.6 Prilog 6 - Tablica za popis uočenih događaja

[C-1] Popis uočenih događaja

Identifikacijska oznaka*	Opis događaja, datum i vrijeme uočavanja, osoba koja je uočila događaj	Potencijalne prijetnje kao posljedica nastanka događaja	Odgovorna osoba za provedbu preventivnih mjera	Poduzete preventivne mjere	Potencijalne buduće prijetnje koje se mogu razviti na temelju događaja

* predlaže se dodjeljivanje identifikacijskih oznaka; primjer identifikacijske oznake: 0001, 0002, 0003 itd.

Vodio/la: _____

12.7 Prilog 7 - Tablica za popis incidenata

[D-1] Popis incidenata

Identifikacijska oznaka*	Opis incidenta, datum i vrijeme odvijanja	Detaljni opis incidenta, zahvaćenih dijelova informacijskog sustava i sudionika (ukoliko su poznati)	Detaljni opis nastale štete	Poduzete mjere oporavka	Potencijalne buduće prijetnje koje se mogu razviti na temelju incidenta	Identifikacijske oznake povezanih događaja s popisa iz mjere C-1	A ***	B ***	C ****	D *****

* predlaže se dodjeljivanje identifikacijskih oznaka; primjer identifikacijske oznake: 0001, 0002, 0003 itd.

** ocjena nastale štete => od 1 do 10 (1 - najmanja šteta, 10 - najveća šteta)

*** ocjena uspješnosti oporavka => od 1 do 10 (1 - spor oporavak, 10 - brz oporavak,)

**** ocjena uspješnosti uklanjanja štete => od 1 do 10 (1 - šteta nije uklonjena, 10 - u potpunosti uklonjena šteta)

***** ukupna ocjena posljedica i oporavka od incidenta => D = B + C - A

Vodio/la: _____

13 Životopis

Alen Šimunic pohađao je osnovnu školu „Braća Radić“ i gimnaziju „Fran Galović“ u Koprivnici, s nastavkom obrazovanja na Ekonomskom fakultetu u Zagrebu. Kroz preddiplomski studij „poslovna ekonomija“ i diplomski studij „menadžerska informatika“, a u uskoj suradnji s Prof. Dr. Sc. Spremićem, stekao je široko znanje o informacijskim sustavima, upravljanju podacima, reviziji informacijskih sustava i primjeni informacijskih sustava u poslovanju. Uz praktična znanja u razvoju *tailor-made* informacijskih sustava ponajviše za mala i srednja poduzeća, u zadnjih 6 godina stekao je stručna znanja o razvoju informacijskih sustava, informacijskoj i kibernetičkoj sigurnosti, forenzici i održavanju informatičke infrastrukture. Kroz praktično iskustvo i obradu tema primjene informacijske tehnologije u poslovanju i informacijske sigurnosti kroz seminarske radove (i završnim radom „Primjena personaliziranih kriptografskih algoritama u poslovanju“), radeći kao demonstrator na katedri za informatiku Ekonomskog fakulteta u Zagrebu i održavajući radionice programiranja u nastavi, stvorio je znanstvene i praktične temelje za izradu okvira za kibernetičku sigurnosti predstavljenog u ovom radu.